ROUTER CONFIGURATION NOTES

路由与交换技术

www.kloudy.cn

2021/6/17

Version 1.0

Preface

> **Kloudy Grasp**: Router Configuration Notes
> 路由与交换技术笔记

1. 说明

Kloudy Grasp: Router Configuration Notes 非官方资料，仅为个人学习笔记，不具有权威性，不完全代表考试内容。

由于是开卷考试，故书本上有的内容就删除了，只留一个页码。
本笔记仅保留重点内容。
本笔记包含三个实验报告文档。

本文内容来自课堂及相关资料，不做任何商业目的，仅供学习交流使用。

2. 版权声明

3. Kloudy Grasp 重要度标识

★ 非常重要
▲ 重要
一般
▽ 不重要
○ 不要求

4. 考试说明

开卷考试
只能带课本
考试题型未知

Content

1 网络技术基础

2 以太网技术及交换机基本配置

2.1 以太网

2.2 二层交换机

2.3 配置二层交换机

(4) 通过 SNMP 管理工作站对交换机进行远程管理

19. 使用命令行接口配置交换机 P43

用户模式
特权模式
配置模式

20. 交换机的基本管理配置 P46

管理系统的日期和时间
系统名称
创建标题
管理地址表 MAC

21. ★交换机接口的基本配置 P50

(1) 交换机接口分类

交换机接口可分为 Access Port 和 Trunk Port：

- Access Port 和 Trunk Port 的配置必须通过 switchport 接口配置命令手动配置。
- 端口为 access port 时，该端口只能属于一个 VLAN，
- 端口为 Trunk port 时，该端口传输属于多个 VLAN 的帧，缺省情况下 Trunk port 将传输所有 VLAN 的帧，可通过设置 VLAN 许可列表来限制 trunk port 传输哪些 VLAN 的帧。

(2) 接口配置命令的使用

(3) 配置接口的速度，双工，流控

(4) 查看交换机的系统和配置信息

2.4 交换机链路聚合

22. 链路聚合（Link Aggregation）P53

多个物理端口捆绑在一起，成为一个逻辑端口

23. CISCO 交换机链路聚合使用两种链路聚合协议

(1) CISCO 私有的 PAGP

- Auto：被动等待对端发送 PAgP 请求，本端不主动发送请求，如果两端的模式都是 Auto，那么将无法形成 EtherChannel。
- Desirable：主动向对端发送 PAgP 请求建立 EtherChannel，对端为 Auto 或 Desirable 都等建立 EtherChannel。
- On：强制跟对端建立 EtherChannel，而不用经过 PAgP 进行协商，注意此模式并不推荐使用。

(2) IEEE 的 LACP

- ON ：强制跟对端建立 EtherChannel
- passive：被动模式，该模式下端口不会主动发送 LACPDU 报文，在接收到对端发送的 LACP 报

文后，该端口进入协议计算状态。

- Active：主动模式，该模式下端口会主动向对端发送 LACPDU 报文，进行 LACP 协议的计算。

24. ★CISCO 交换机链路聚合配置 P54

(1) 在接口中设置链路聚合

Sw1(config)#interface range f0/23-24
Sw1(config-if-range)#**channel-group 1 mode on**
Sw2(config)#interface range f0/23-24
Sw2(config-if-range)#channel-group 1 mode on

(2) 进入捆绑组，设置聚合口的接口类型（如果不指定接口类型，会自动继承物理口的类型）

Sw1(config)#**interface port-channel 1**
Sw1(config-if)#switchport trunk encapsulation dot1q （三层）
Sw1(config-if)#switchport mode trunk
Sw1(config-if)#switchport trunk allow vlan all

(3) 查看聚合接口状态

Sw1(config)#do show etherchannel summary
Sw1#show interface etherchannel

(4) 删除端口聚合

Sw1(config)#no interface port-channel 1

2.5 生成树协议

25. 生成树协议 P55

解决问题：交换网络内的冗余拓扑
作用：减少单点故障，增加网络可靠性

产生交换环路，会导致：

- 广播风暴
- 多帧复制
- MAC 地址表抖动

26. ★生成树协议配置 P58

(1) 恢复缺省配置

Switch(config)# **spanning-tree reset** (PT 模拟器不支持)

(2) 打开、关闭 STP

Switch(config)# **spanning-tree mode *pvst***
Switch(config)# no spanning-tree mode

(3) 修改生成树协议的类型

Switch(config)#**spanning-tree mode** *{mstp|stp|rstp|pvst|rapid-pvst}*

cisco 交换机默认是 pvst

(4) 在 VLAN 上启用生成树

Switch(config)#**spanning-tree vlan** *1*

Switch(config-if)#**spanning-tree vlan** *1*

(5) 配置交换机的优先级

Switch(config)#**spanning-tree vlan** *1* **priority** *<0-61440>* (模拟器不支持)

注意：网桥优先级配置只能为 4096 的倍数

Cisco 模拟器支持，如下图

```
Switch(config)#spanning-tree ?
  mode      Spanning tree operating mode
  portfast  Spanning tree portfast options
  vlan      VLAN Switch Spanning Tree
Switch(config)#spanning-tree vl
Switch(config)#spanning-tree vlan ?
  WORD  vlan range, example: 1,3-5,7,9-11
Switch(config)#spanning-tree vlan 1 ?
  priority  Set the bridge priority for the spanning tree
  root      Configure switch as root
  <cr>
Switch(config)#spanning-tree vlan 1 pri
Switch(config)#spanning-tree vlan 1 priority ?
  <0-61440>  bridge priority in increments of 4096
Switch(config)#spanning-tree vlan 1 priority  128 ?
  <cr>
Switch(config)#spanning-tree vlan 1 priority  128
Ctrl+F6 to exit CLI focus
```

错误 4096倍数

(6) 配置端口的优先级

Switch(config-if)#**spanning-tree vlan** *1* **port-priority** *<0-240>*

注意：端口优先级配置只能为 16 的倍数

模拟器操作如下图所示

```
Switch(config-if)#spanning-tree ?
  bpduguard  Don't accept BPDUs on this interface
  cost       Change an interface's spanning tree port path cost
  guard      Change an interface's spanning tree guard mode
  link-type  Specify a link type for spanning tree protocol use
  portfast   Enable an interface to move directly to forwarding on
  vlan       VLAN Switch Spanning Tree
Switch(config-if)#spanning-tree vl
Switch(config-if)#spanning-tree vlan ?
  WORD  vlan range, example: 1,3-5,7,9-11
Switch(config-if)#spanning-tree vlan 1 ?
  cost           Change an interface's spanning tree port path cost
  port-priority  Change an interface's spanning tree port priority
Switch(config-if)#spanning-tree vlan 1
```

(7) 配置端口的路径成本

Switch(config-if)#**spanning-tree cost** *cost*

(8) 配置端口路径成本的默认计算方法

Switch(config)#**spanning-tree path-cost method** *{long|short}*

注意：默认值为长整型（long）

(9) 配置 Hello Time、Forward-delay Time 和 Max-age Time （模拟器不支持）

Switch(config)#**spanning-tree hello-time|forward-time|max-age** *seconds*

(10) 配置链路类型 （模拟器不支持）

Switch(config-if)#**spanning-tree link-type** *{point-to-poin|shared}*

(11) 查看生成树的配置

Switch#**show spanning-tree**

Switch#**show spanning-tree interface** *interface-id*

2.6 系统日志管理

---

27. 系统日志管理 P59

3 虚拟局域网 VLAN

3.1 VLAN

28. 分割广播域 P62

交换网络是平面网络结构，必须依赖广播。

广播域过大会导致：

- 带宽浪费
- 安全性降低
- 不易管理

分割广播域的方法：

- 使用路由器连接多个子网
- 使用虚拟局域网 VLAN

29. 虚拟局域网（Virtual Local Area Network，VLAN） P62

VLAN 的特点：

- 基于逻辑的分组
- 不受物理位置限制
- 在同一 VLAN 内和真实局域网相同
- 不同 VLAN 内用户要通信需要借助三层设备

VLAN 的用途：

- 控制不必要的广播报文的扩散
- 提高网络带宽利用率，减少资源浪费
- 划分不同的用户组，对组之间的访问进行限制
- 增加安全性

VLAN 的优点：

- 限制广播包
- 安全性
- 虚拟工作组
- 减少移动和改变的代价

30. VLAN 的定义方法 P63

(1) 基于端口的 VLAN

根据以太网交换机的端口来划分

(2) 基于 MAC 地址的 VLAN

根据每个主机网卡的 MAC 地址来划分

(3) 基于网络层的 VLAN

根据每个主机的网络层地址或协议类型（如果支持多协议）划分的

(4) 基于 IP 组播的 VLAN

一个组播组就是一个 VLAN

31. VLAN 中继协议 P64

3.2 ★基于端口的 VLAN 配置 P66

32. 交换机端口

交换机上的二层接口成为 Switch port，只有二层交换功能

- **ACCESS 端口**
  UnTagged 端口，即接入端口
  Access 端口只能属于一个 VLAN，它发送的帧不带有 VLAN 标签，一般用于连接计算机的端口

- **Trunk 端口**
  Tag Aware 端口，即干道接口
  可以允许多个 VLAN 通过，它发出的帧一般是带有 VLAN 标签的，一般用于交换机之间连接的端口

33. 802.1Q 的缺省 VLAN

一个 802.1Q 的 Trunk 端口有一个缺省 VLAN 的 ID 值（VLAN 1）
802.1Q 不为缺省 VLAN 的帧打标签

34. VLAN 定义的步骤

1. 首先添加 VLAN
2. 为端口分配 VLAN （使用命令 interface 选择接口，接口模式下分配该接口为哪一 VLAN)
3. 跨交换机的 VLAN 通信，配置 Trunk 口
4. 使用 show vlan 等命令进行验证或查看 VLAN 配置，使用 show run 查看当前交换机正在运行的配置

35. VLAN 的配置

(1) 添加或者修改 VLAN

Switch# conf t
Switch(config)# vlan *vlan-id*
Switch(config-vlan)# name *vlan-name*

(2) 删除 VLAN

Switch(config)# no vlan *vlan-id*

(3) 查看 VLAN

Switch#show vlan

36. 将端口分配给一个 VLAN

Switch(config)# **interface** *interface-id*
Switch(config)# **interface range {***port-range***}**
Switch(config-if)# **switchport mode access**
Switch(config-if)# **switchport access vlan** *vlan-id*

VLAN ID	范围	用途	是否通过VTP传播
0和4095	保留	用户不能使用	不适用
1	常规范围	默认VLAN，不可删除	是
2-1000	常规范围	用户能够创建、使用和删除	是
1001	常规范围	用户不能创建、使用和删除	是
1002-1005	保留	FDDI和令牌环	不适用
1006-1009	保留		不适用
1010-1024	保留		不适用
1025-4094	保留	有限使用	否

37. 配置 VLAN Trunk

(1) 将端口设置成 Trunk 端口

Switch(config)# **interface** *interface-id*
Switch(config-if)#**switchport mode trunk** 配置为 trunk
Switch(config-if)#no **switchport mode** 删除 trunk 配置

(2) 指定 Trunk 端口的缺省 VLAN

Switch(config-if)#**switchport trunk native vlan** *vlan-id*

默认的缺省 VLAN 是 VLAN 1,也就是在 trunk 线路不给该 VLAN 打 VLAN ID 标记
Trunk 链路两端必须一致的 natvie VLAN ID,否这会错误异常

38. show …

(1)

Switch#show vlan

```
VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1 ,Fa0/2 ,Fa0/3 , Fa0/4 ,Fa0/6 ,Fa0/9
                                                   Fa0/16,Fa0/17,Fa0/18 ,
Fa0/19,Fa0/20,Fa0/21
                                                   Fa0/22,Fa0/23,Fa0/24
10   gongcheng                           active    Fa0/1 ,Fa0/5 ,Fa0/7
20   xiaoshou                            active    Fa0/1 ,Fa0/8 ,Fa0/10 ,Fa0/11,Fa0/12,Fa0/13
                                                   Fa0/14,Fa0/15
```

(2)

Switch#show interfaces fastEthernet 0/1 switchport

```
Interface    Switchport Mode         Access    Native      Protected VLAN lists
---------- ---------- --------- ------- -------- --------- --------------------
Fa0/1          Enabled      Trunk        1           1            Disabled    All
```

(3)

Switch#show interfaces fastEthernet 0/1 trunk

```
Interface                  Mode      Native VLAN VLAN lists
-------------------- ------ ----------- --------------------
Fa0/1                       On        1              All
```

4 交换机安全配置交换机安全配置

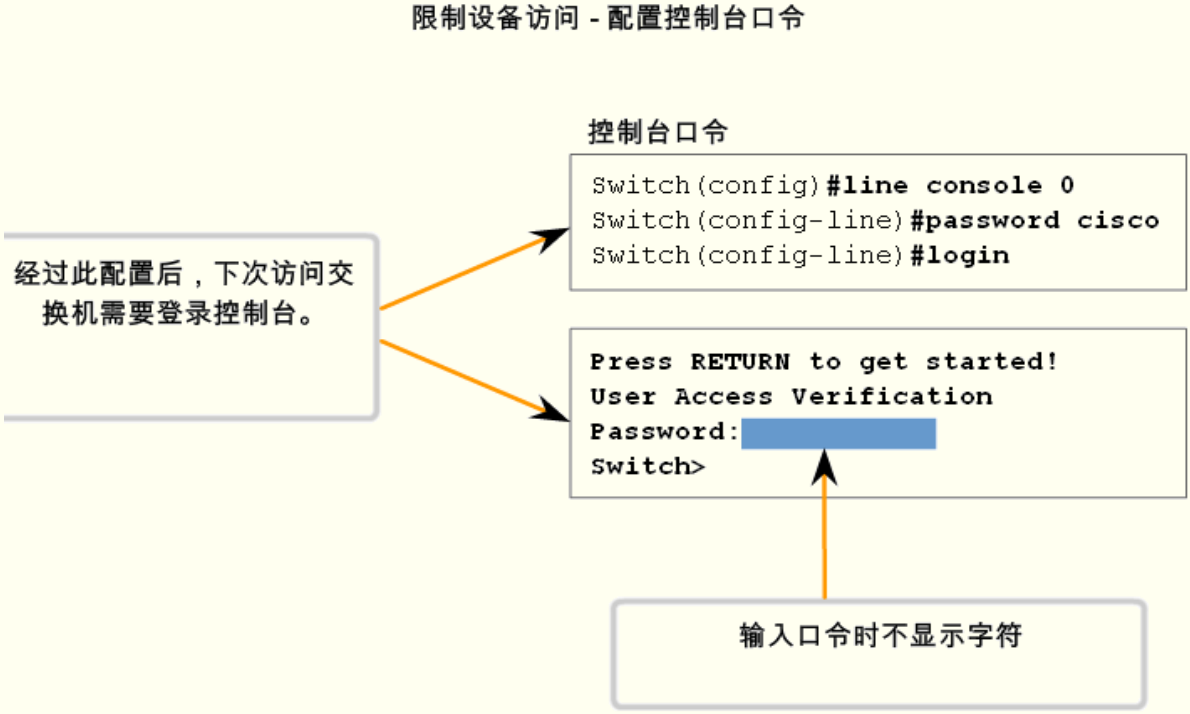
4.1 终端访问安全

39. 配置口令

控制台 console 口令 — 用于限制人员通过控制台连接访问设备
使能 enable 口令 — 用于限制人员访问特权执行模式
使能 enable 加密口令 — 经加密，用于限制人员访问特权执行模式
VTY 口令 — 用于限制人员通过 Telnet 访问设备

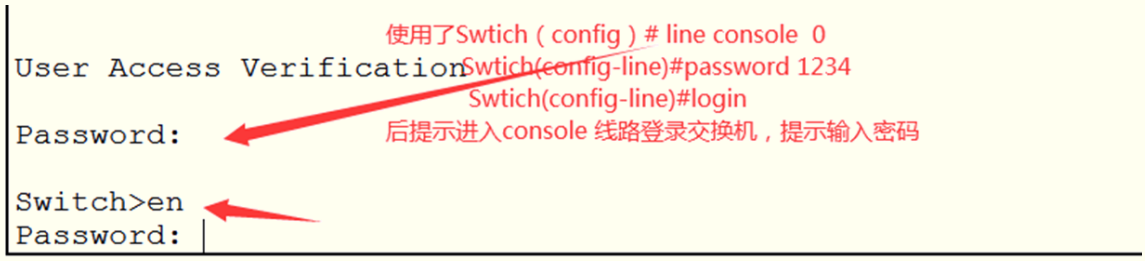
40. 配置控制台 console 口令 P78

Switch(config)#line console 0
Switch(config-line)#password *password*
Switch(config-line)#login



41. 配置使能 enable 口令 P80

Swtich(config)#enable password *password*
Swtich(config)#enable secret *password*



请尽可能使用 enable secret 命令，而不要 使用较老版本的 enable password 命令。enable secret 命令可提供更强的安全性，因为使用此命令设置的口令会被加密。enable password 命令仅在尚未使用 enable secret 命令设置口令时才能使用。

42. 配置 VTY（Telnet 远程连接）口令 P81

Swtich(config)#line vty 0 4
Swtich(config-line)#password *password*
Swtich(config-line)#login
Switch(config)#int vlan 1
Switch(config-if)#ip addr 192.168.1.1 255.255.255.0 #设置管理地址
Switch(config-if)#no shutdown #开启端口 up

```
Switch#conf t
Enter configuration commands, one per line.  End wit
Switch(config)#line vt
Switch(config)#line vty 0 4
Switch(config-line)#password cisco
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#enable password cisco
Switch(config)#end
Switch#
```

43. 加密显示口令

它可在用户配置口令后使口令加密显示。service password-encryption 命令对所有未加密的口令进行弱加密。当通过介质发送口令时，此加密手段不适用，它仅适用于配置文件中的口令。此命令的用途在于防止未经授权的人员查看配置文件中的口令。

Swtich(config)# **service password-encryption**

44. 配置特权等级 P82

用户级别范围是 0~15 级，级别 0 是最低的级别。
交换机设备系统只有两个受口令保护的授权级别：普通用户级别（0 级）和特权用户级别（15 级）。

4.2 交换机端口安全控制

4.3 实验一 交换机安全配置及 VLAN 配置

【实验目的】

1、回顾原来的交换机的基本配置命令,比如 show run、write、conf t、interface 接口命令，以及交换机的管理地址配置。

2、完成和掌握交换机的交换机管理 IP 配置、接口的配置、口令的配置、端口安全性、VLAN 和跨交换机 VLAN 的配置、冗余链路配置。并验证其网络连通性，并能够熟练使用类似的 show vlan 、ping、write、hostname 命令完成交换机的基本操作。

。

【实验环境】

Cisco PacketTracer 7.2 及以上版本模拟器软件，

下载位置：https://www.netacad.com/portal/resources/packet-tracer（需要注册下载）或者 在 jxpt.cuit.edu.cn 中下载

【实验内容及步骤】

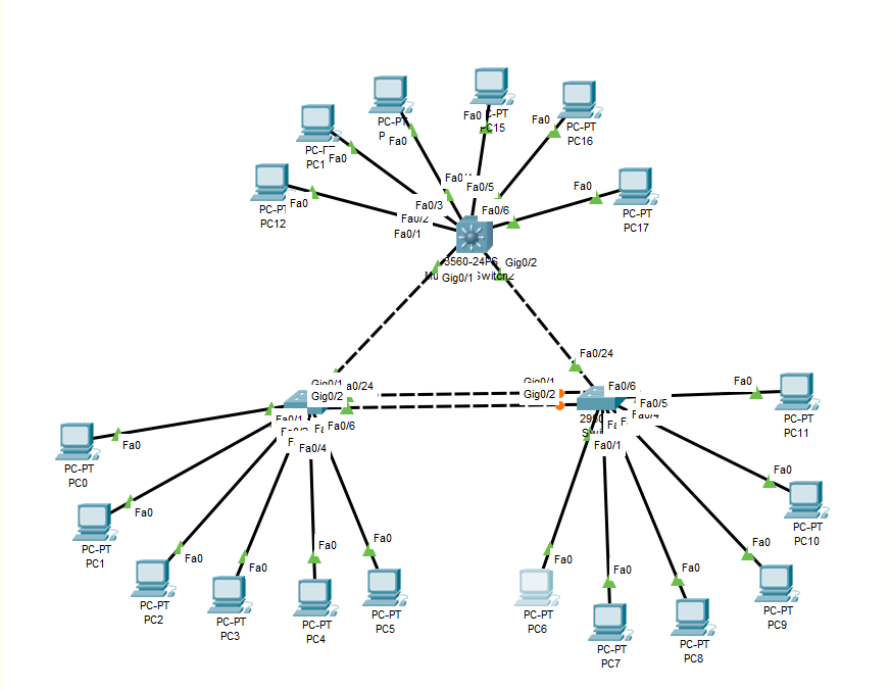
内容要求：

某实验室，有 54 台 PC 主机，需要分成 6 组，每一组的 PC 主机 9 台，需要选用 1 台 Cisco3560 三层交换机，选用 2 台 2950 交换机，构成实验室局域网 ，每一台交换机的物理端口都连接了 6 组的 PC 主机，请使用 Packet Tracer 模拟器设计一个网络，有 6 个 VLAN ，每一台交换机都有 6 个 VLAN ，并且每一 VLAN 用一 PC 主机模拟就可以，完成跨交换机的同一 VLAN 传输通信。配置中，应实现端口的一些安全配置，实现每一交换机配置管理 IP 地址和主机名，实现交换机之间两两相互连接来实现冗余链路配置，开启 PVST+生成树协议，实现跨交换机的同一 VLAN 通信。

1.实验拓扑图

（根据实验要求，使用 Packet tracer 完成实验拓扑）

选用 1 台 Cisco3560 三层交换机，选用 2 台 2950 交换机，每一台交换机都有 6 个 VLAN，每一 VLAN 用一 PC 主机模拟：



2. 主要操作过程

第一，打开软件，进入操作主界面，进行布局拓扑图

第二，规划 IP 地址或 VLAN 地址

局域网 1：192.168.10.0/24 网段

PC0 IP 192.168.10.1， 子网掩码 255.255.255.0， 网关 0.0.0.0

PC6 IP 192.168.10.2， 子网掩码 255.255.255.0， 网关 0.0.0.0

PC12 IP 192.168.10.3， 子网掩码 255.255.255.0， 网关 0.0.0.0

局域网 2：192.168.20.0/24 网段

PC1 IP 192.168.20.1， 子网掩码 255.255.255.0， 网关 0.0.0.0

PC7 IP 192.168.20.2， 子网掩码 255.255.255.0， 网关 0.0.0.0

PC13 IP 192.168.20.3， 子网掩码 255.255.255.0， 网关 0.0.0.0

局域网 3：192.168.30.0/24 网段

PC2 IP 192.168.30.1， 子网掩码 255.255.255.0， 网关 0.0.0.0

PC8 IP 192.168.30.2， 子网掩码 255.255.255.0， 网关 0.0.0.0

PC14 IP 192.168.30.3， 子网掩码 255.255.255.0， 网关 0.0.0.0

局域网 4：192.168.40.0/24 网段

PC3 IP 192.168.40.1， 子网掩码 255.255.255.0， 网关 0.0.0.0

PC9 IP 192.168.40.2， 子网掩码 255.255.255.0， 网关 0.0.0.0

PC15 IP 192.168.40.3， 子网掩码 255.255.255.0， 网关 0.0.0.0

局域网 5：192.168.50.0/24 网段

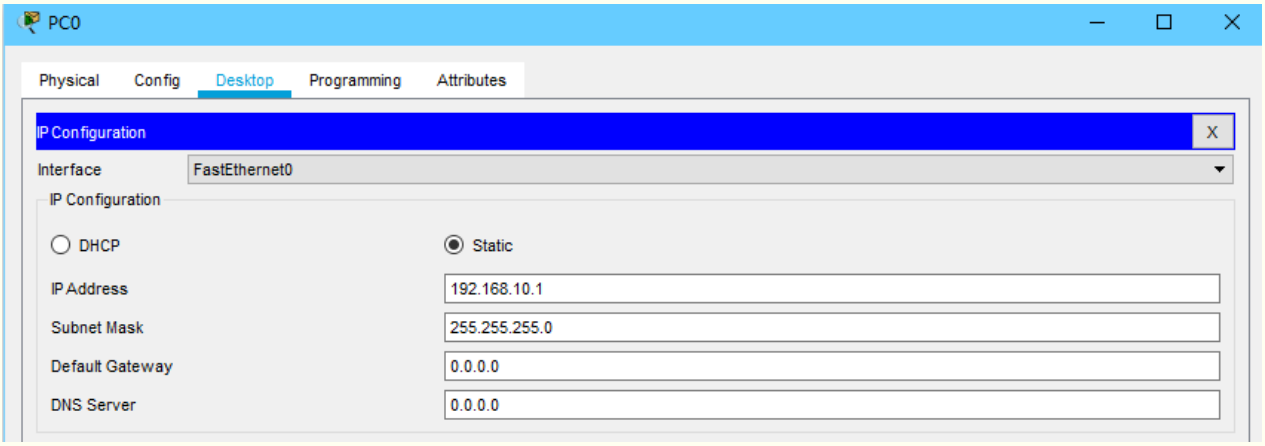
PC4 IP 192.168.50.1， 子网掩码 255.255.255.0， 网关 0.0.0.0

PC10 IP 192.168.50.2， 子网掩码 255.255.255.0， 网关 0.0.0.0

PC16 IP 192.168.50.3， 子网掩码 255.255.255.0， 网关 0.0.0.0

局域网 6：192.168.60.0/24 网段
PC5 IP 192.168.60.1， 子网掩码 255.255.255.0， 网关 0.0.0.0
PC11 IP 192.168.60.2， 子网掩码 255.255.255.0， 网关 0.0.0.0
PC17 IP 192.168.60.3， 子网掩码 255.255.255.0， 网关 0.0.0.0

第三，通过窗口配置各个 PC 主机的 IP 地址，方法如下图所示。



其余 17 个主机类似。

第四，配置交换机

配置交换机 0 的内容如下：

创建 VLAN：

enable	进入特权模式
config terminal	进入全局模式
vlan 10	创建 VLAN10（依次类推创建直到 VLAN60）

```
Switch>enable
Switch#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#vlan 30
Switch(config-vlan)#vlan 40
Switch(config-vlan)#vlan 50
Switch(config-vlan)#vlan 60
Switch(config-vlan)#
```

将端口添加到 VLAN 中：

interface Fa0/1	选择端口 Fa0/1
switchport mode access	定义该端口的 VLAN 成员类型（Access）
switchport access vlan 10	将端口添加到 VLAN10 中

```
Switch(config)#int Fa0/1
Switch(config-if)#sw mode acc
Switch(config-if)#sw acc vlan 10
```

（重复以上三步，将六个端口添加到六个 VLAN 中）

```
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23
10   VLAN0010                          active    Fa0/1
20   VLAN0020                          active    Fa0/2
30   VLAN0030                          active    Fa0/3
40   VLAN0040                          active    Fa0/4
50   VLAN0050                          active    Fa0/5
60   VLAN0060                          active    Fa0/6
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
50   enet  100050     1500  -      -      -        -    -        0      0
60   enet  100060     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

配置跨交换机端口：

interface Fa0/24	选择端口 Fa0/24
switchport mode trunk	定义该端口的 VLAN 成员类型（Trunk）

```
Switch(config)#int Fa0/24
Switch(config-if)#sw mode trunk
```

配置跨交换机聚合端口：

interface port-channel 1	创建 AP 号
interface range Gig0/1, Gig0/2	选择端口 Gig0/1, Gig0/2
channel-group 1 mode on	设置 AP 号
interface port-channel 1	选择 AP 号
switchport mode trunk	定义该端口的 VLAN 成员类型（Trunk）

```
Switch(config)#interface port-channel 1
Switch(config-if)#interface range Gig0/1, Gig0/2
Switch(config-if-range)#channel-group 1 mode on
Switch(config-if-range)#interface port-channel 1
Switch(config-if)#switchport mode trunk
```

配置快速生成树：

spanning-tree mode rapid-pvst 配置快速生成树

```
Switch(config)#spanning-tree mode rapid-pvst
```

配置交换机 1 的内容如下：

创建 VLAN、将端口添加到 VLAN 中同交换机 0：

```
Switch>en
Switch#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#vlan 30
Switch(config-vlan)#vlan 40
Switch(config-vlan)#vlan 50
Switch(config-vlan)#vlan 60
Switch(config-vlan)#int Fa0/1
Switch(config-if)#sw mode acc
Switch(config-if)#sw acc vlan 10
```

```
Switch#show vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                   Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                   Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                   Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                   Fa0/23, Gig0/2
10   VLAN0010                            active    Fa0/1
20   VLAN0020                            active    Fa0/2
30   VLAN0030                            active    Fa0/3
40   VLAN0040                            active    Fa0/4
50   VLAN0050                            active    Fa0/5
60   VLAN0060                            active    Fa0/6
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
50   enet  100050     1500  -      -      -        -    -        0      0
60   enet  100060     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

配置跨交换机端口：

interface Fa0/24	选择端口 Fa0/24
switchport mode trunk	定义该端口的 VLAN 成员类型（Trunk）

```
Switch(config)#int Fa0/24
Switch(config-if)#sw mode trunk
```

配置跨交换机聚合端口：

interface port-channel 1	创建 AP 号
interface range Gig0/1, Gig0/2	选择端口 Gig0/1, Gig0/2
channel-group 1 mode on	设置 AP 号
interface port-channel 1	选择 AP 号
switchport mode trunk	定义该端口的 VLAN 成员类型（Trunk）

```
Switch(config)#interface port-channel 1
Switch(config-if)#interface range Gig0/1, Gig0/2
Switch(config-if-range)#channel-group 1 mode on
Switch(config-if-range)#interface port-channel 1
Switch(config-if)#switchport mode trunk
```

配置交换机 2 的内容如下：

创建 VLAN、将端口添加到 VLAN 中同交换机 0：

```
Switch(config)#vlan 10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#vlan 30
Switch(config-vlan)#vlan 40
Switch(config-vlan)#vlan 50
Switch(config-vlan)#vlan 60
Switch(config-vlan)#int Fa0/1
Switch(config-if)#sw mode acc
Switch(config-if)#sw acc vlan 10
Switch(config-if)#int Fa0/2
Switch(config-if)#sw mode acc
Switch(config-if)#sw acc vlan 20
```

```
Switch#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                 Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                 Fa0/23, Fa0/24
10   VLAN0010                          active    Fa0/1
20   VLAN0020                          active    Fa0/2
30   VLAN0030                          active    Fa0/3
40   VLAN0040                          active    Fa0/4
50   VLAN0050                          active    Fa0/5
60   VLAN0060                          active    Fa0/6
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
50   enet  100050     1500  -      -      -        -    -        0      0
60   enet  100060     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

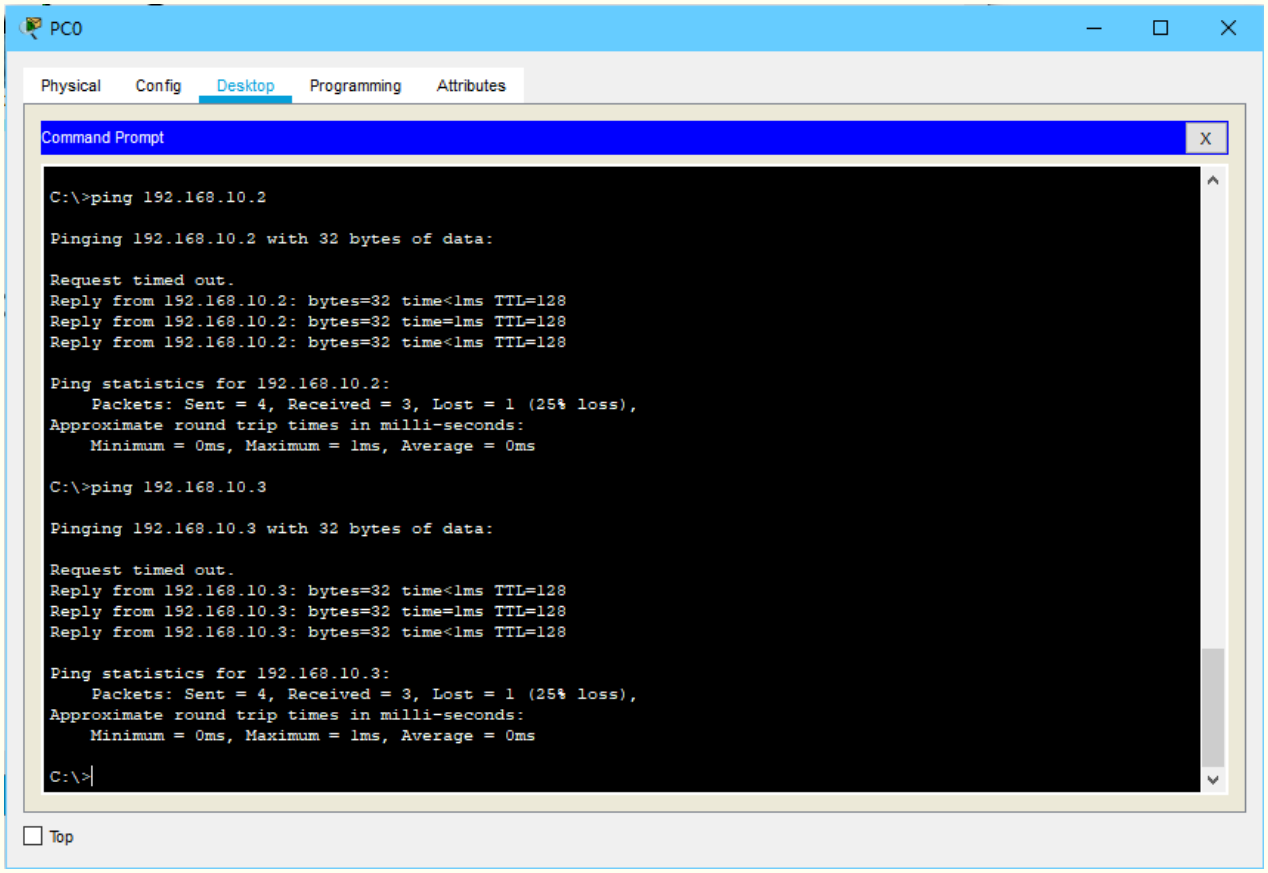
配置跨交换机端口：

interface Gig0/1	选择端口 Gig0/1
switchport mode trunk	定义该端口的 VLAN 成员类型（Trunk）

interface Gig0/2 选择端口 Gig0/2
switchport mode trunk 定义该端口的 VLAN 成员类型（Trunk）

```
Switch(config-if)#int Gig0/1
Switch(config-if)#sw mode trunk
Switch(config-if)#int Gig0/2
Switch(config-if)#sw mode trunk
```

第五，验证配置结果
在 PC0 中启动 CMD 窗口，通过 ping 来验证，结果如下图



在 PC6 和 PC12 中类似。
结论：同一 VLAN 的 PC 可以 ping 通，说明 VLAN 配置成功。

在交换机 0 中，通过命令 show run 查看端口配置是否生效

```
Switch#show run
Building configuration...

Current configuration : 1558 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
interface Port-channel1
 switchport mode trunk
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 60
 switchport mode access
!
```

```
interface FastEthernet0/24
 switchport mode trunk
!
interface GigabitEthernet0/1
 switchport mode trunk
 channel-group 1 mode on
!
interface GigabitEthernet0/2
 switchport mode trunk
 channel-group 1 mode on
!
```

在交换机 0 中，通过命令 show int 查看配置名验证是否生效

```
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (VLAN0010)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

```
Name: Fa0/24
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

```
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: All
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

在交换机 0 中，通过命令 show span 查看生成树情况

```
Switch#show span
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0005.5E54.24AC
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0005.5E54.24AC
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Po1              Desg FWD 3         128.27   Shr
Fa0/24           Desg FWD 19        128.24   P2p

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    32778
              Address     0005.5E54.24AC
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0005.5E54.24AC
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/24           Desg FWD 19        128.24   P2p
```

交换机 1 和 2 类似。

【实验结论或实验体会】

通过本次实验,理解了路由、交换机、VLAN、端口聚合、生成树等的概念,熟悉了 VLAN 配置，以及 show、int、sw、acc、trunk、exit、write 等命令的使用,遇到了三层交换机无法 trunk 的问题,通过查阅资料,发现该问题可以通过 switchport trunk encapsulation dot1q 解决。遇到了 Translating ..... domain server 的问题,通过查阅资料,发现该问题可以通过 no ip domain-look up 解决。

5 网络互连技术及路由器基本配置

5.1 网络互连技术

49. 路由器 P107

50. 路由器转发 IP 包 P113

5.2 路由器基本配置

51. 常见路由器配置方式 P117

- 利用终端通过 Console 口进行本地配置；
- 通过 telnet 方式进行本地或者远程配置；
- 预先编辑好配置文件，通过 TFTP 方式进行网络配置；
- 通过 web 页面进行配置。

52. 路由器基本配置 P122

53. ★路由器接口配置 P131

ip add 配置 IP 地址

no sh

54. 路由器口令配置 P134

55. ★VLAN 间路由（单臂路由） P136

(1) 配置链路类型

```
SW1(config)#inter f0/1
SW1(config-if)#switchport access vlan 10

SW1(config)#inter f0/2
SW1(config-if)#switchport access vlan 20

SW1(config)#inter f0/24
SW1(config-if)#switchport mode trunk
```

(2) 配置 VLAN 标签的封装结构

```
R1(config)#inter f0/0.1
R1(config-subif)#encapsulation dot1Q 10

R1(config)#inter f0/0.2
R1(config-subif)#encapsulation dot1Q 20
```

子接口对应的 VLAN

(3) 配置子接口地址

R1(config)#inter f0/0.1
R1(config-subif)#ip add **10.0.0.1 255.255.255.0**

R1(config)#inter f0/0.2
R1(config-subif)#ip add **20.0.0.1 255.255.255.0**

子接口对应 VLAN 的网关地址

6 路由协议及配置

56. 路由表 P139

在 Cisco IOS 路由器上，show ip route 命令可用于显示路由器 IPv4 路由表。

6.1 静态路由配置

57. 静态路由配置

配置静态路由的命令是 ip route。配置静态路由的完整语法是:

Router(config)#**ip route *network-address subnet-mask* {ip-address | exit-interface }**

参数	描述
network-address	要加入路由表的远程网络的目的网络地址。
subnet-mask	要加入路由表的远程网络的子网掩码。可对此子网掩码进行修改，以总结一组网络。
ip-address | exit-interface	一般指下一跳路由器的 IP 地址|将数据包转发到目的网络时使用的送出接口

```
RB>enable
RB#configure terminal
RB（config）#ip route 172.1.1.0 255.255.255.0 172.1.2.1
(或 ip route 172.1.1.0 255.255.255.0 serial 1/2)
RB（config）#end
```

58. 缺省路由配置

缺省路由一般使用在 stub 网络中（称末端或存根网络），stub 网络是只有 1 条出口路径的网络。

```
router(config)#ip route 0.0.0.0 0.0.0.0 [转发路由器的 IP 地址/本地接口]

router(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

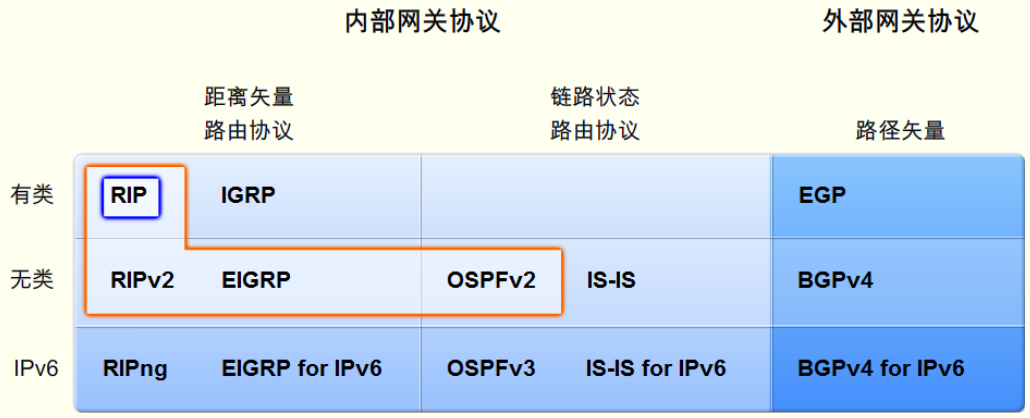
6.2 ★动态路由配置

59. 路由协议可以按照以下内容分类

目的：内部网关协议（IGP）或外部网关协议（EGP）

操作：距离矢量、链路状态协议或路径矢量协议

行为：有类协议（传统）或无类协议



60. 动态路由协议相对于静态路由协议

	动态路由	静态路由
配置的复杂性	通常不受网络规模限制	随着网络规模的增大而愈趋复杂
管理员所需知识	需要掌握高级的知识和技能	不需要额外的专业知识
拓扑结构变化	自动根据拓扑结构变化进行调整	需要管理员参与
可扩展性	简单拓扑结构和复杂拓扑结构均适合	适合简单的网络拓扑结构
安全性	不够安全	更安全
资源使用情况	占用 CPU、内存和链路带宽	不需要额外的资源
可预测性	根据当前网络拓扑结构确定路径	总是通过同一路径到达目的网络

61. 管理距离

(1) 度量的用途

用于确定到达目的的最佳路径

(2) 管理距离的用途

这个数值用于指定路由协议的优先级

对于路由表条目，括号中的第一个值即为 AD 值

路由来源	管理距离
相连	0
静态	1
EIGRP 总结路由	5
外部 BGP	20
内部 EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
外部 EIGRP	170
内部 BGP	200

6.2.1 RIP

62. RIP 协议 P143

63. 配置 RIP P145

(1) RIPv1

步骤	命令	功能
步骤1	Router(config)#router rip	创建RIP路由进程
步骤2	Router(config-router)#network *directly-connected-classful-network-address*	定义关联网络，在特定网络所属的所有接口上启用 RIP。 输入参数为每个直连网络的有类网络地址。

(2) RIPv2

步骤	命令	功能
步骤1	Router(config)#**router rip**	创建RIP路由进程
步骤2	Router(config-router)# **version 2**	将RIP版本修改为使用第 2 版。
步骤3	Router(config-router)#**network** *directly-connected-classful-network-address*	定义关联网络，在特定网络所属的所有接口上启用 RIP。 输入参数为每个直连网络的有类网络地址。

```
步骤 1：配置路由器 R1
R1(config)#router rip                          //启动 RIP 进程
R1(config-router)#version 1                    //配置 RIP 版本 1
R1(config-router)#network 1.0.0.0              //通告网络
R1(config-router)#network 192.168.12.0
步骤 2：配置路由器 R2
R2(config)#router rip
R2(config-router)#version 1
R2(config-router)#network 192.168.12.0
R2(config-router)#network 192.168.23.0
步骤 3：配置路由器 R3
R3(config)#router rip
R3(config-router)#version 1
R3(config-router)#network 192.168.23.0
R3(config-router)#network 192.168.34.0
```

64. 关闭路由自动汇聚 P146

命令	作用
Router(config-router)#**no auto-summary**	关闭路由自动汇总
Router(config-router)#**auto-summary**	打开路由自动汇总

6.2.2 OSPF

65. OSPF 协议 P148

66. 创建 OSPF 路由进程 P150

注意使用通配符掩码而不是子网掩码

步骤	命令	含义
步骤1	Router# **configure terminal**	进入全局配置模式。
步骤2	Router(config)# **router ospf** *process-id*	打开OSPF，进入OSPF配置模式，process-id指的是进程号，指定范围在1-65535， process-id只在路由器内部起作用，不同路由器的process-id可以不同
步骤3	Router(config-router)# **network** *address wildcard-mask area area-id*	命令决定了哪些接口参与OSPF 区域的路由过程。路由器上任何匹配network命令中的网络地址的接口都将启用，可发送和接收 OSPF 数据包。
步骤4	Router(config-router)# **end**	退回到特权模式。
步骤5	Router# **show ip protocol**	显示当前运行的路由协议。
步骤6	Router# **write**	保存配置。

```
Router (config)# router ospf 10
Router (config-router)# network 192.168.0.0  0.0.0.255 area 0
Router (config-router)# end
```

7 三层交换机

67. 应该不考

具体看书

8 路由器安全配置

8.1 终端访问安全配置

68. 配置控制台访问口令

Switch(config)# #line con 0
Switch(config-line)# password *cisco*

69. 配置虚拟终端访问口令

Switch(config) #line vty 0 4
Switch(config-line)# password *cisco*
Switch (config-line)#login

70. 登录密码设置

Switch(config)# enable password *password*

71. 配置和管理 SSH

72. 终端访问限制

#line vty 0 4
exec-timeout *seconds*
login local

73. 配置特权等级

Switch(config)# enable secret [level *level*] { password }
username *username* privilege *level* password *password*
privilege *mode* level *level command*

8.2 网络服务管理

74. 网络服务管理 P181

具体看书

8.3 路由协议安全

75. 启用 RIPv2 身份验证 P184

步骤 1：在路由器模式下配置一个密钥链（key-chain），一个密钥链可以包含多个密钥。
router(config)# key chain *key-chain-name*
密钥链名称

步骤 2：定义密钥编号。
router(config-keychain)# key *key-number*

密钥编号<0-2147483647>。

步骤 3：定义密钥。
Router(config-keychain-key)# key-string *string*
string：密钥字符串。执行验证的双方密钥字符串必须一致。

步骤 4：在需要执行路由信息验证更新的接口上应用密钥链。 (模拟器不支持)
router(config-if)#ip rip authentication *key-chain key-chain-name*
key-chain-name：使用的密钥链名称。
以上配置是明文验证需要配置的内容，即默认验证方法。如果需要密文验证，则要附加下面的命令：

步骤 5：声明验证模式。
router(config-if)#ip rip authentication mode md5
验证 MD5 身份验证：
使用 debug ip rip 命令可以观察验证是否成功的信息。

76. 启用 OSPF 身份验证 P186

Router1 配置：

```
Router1# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)# router ospf 1
Router1(config-router)# network 14.1.0.0 0.0.255.255 area 0
! 启用 MD5 认证。
Router1(config-router)# area 0 authentication message-digest
Router1(config-router)# exit
Router1(config)# int eth0/1
！启用 MD5 密钥 Key 为 ospfkey。
Router1(config-if)# ip ospf message-digest-key 1 md5 ospfkey
Router1(config-if)# end
Router1#
```

Router2 配置：

```
Router2# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router2(config)# router ospf 1
Router2(config-router)# area 0 authentication message-digest
Router2(config-router)# network 14.1.0.0 0.0.255.255 area 0
Router2(config-router)# network 14.2.6.0 0.0.0.255 area 0
Router2(config-router)# exit
Router2(config)# int eth0
Router2(config-if)# ip ospf message-digest-key 1 md5 ospfkey
Router2(config-if)# end
```

验证 MD5 身份验证：

使用 show ip ospf interface 命令可以查看为接口配置的身份验证类型，如此输出所示。这里，已配置了 Serial 0 接口以使用密钥 ID“1”进行 MD5 身份验证。

8.4 使用网络加密

77. Ipsec 协议 P189

VPN 配置

8.5 实验二 路由器安全配置与路由技术

【实验目的】

1、熟练路由器的基本配置,路由器配置模式、工作时间、名字，路由器各类接口 IP 地址的配置和启用、各种口令的配置。

2、利用静态路由和 RIPV1、V2、OSPF 动态路由实现多个网络之间的路由功能。

3、分别利用路由器和三层交换机实现网络的互连互通。

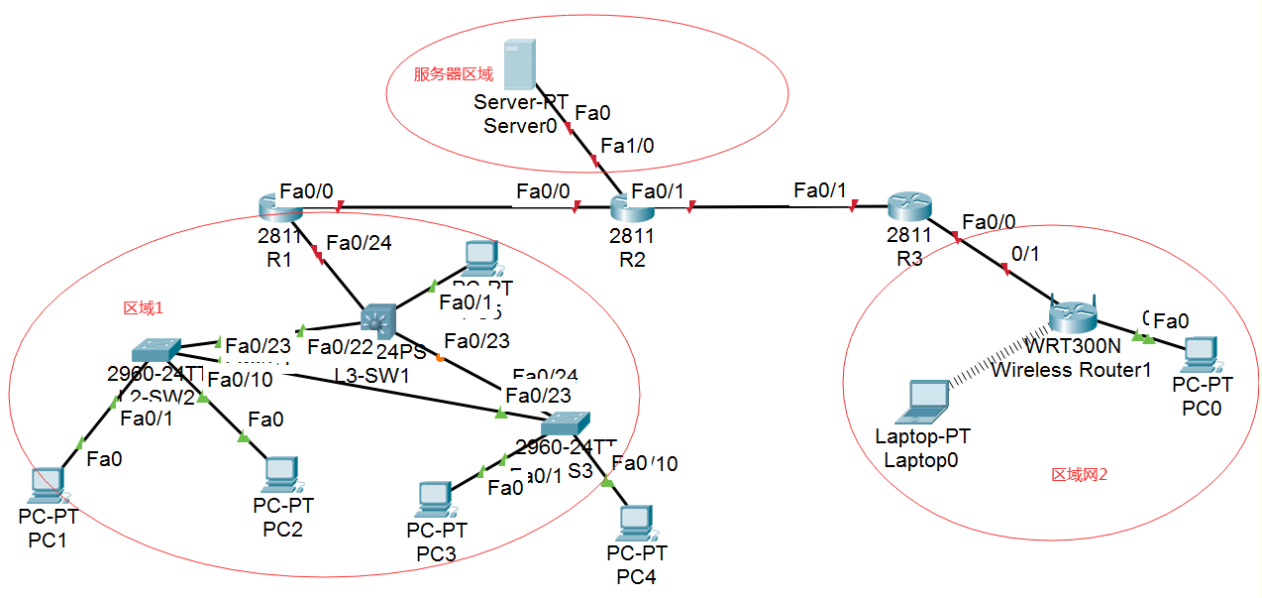
【实验环境】

Cisco PacketTracer 7.2 及以上模拟器软件

下载位置：https://www.netacad.com/portal/resources/packet-tracer（需要注册下载）或者 在 jxpt.cuit.edu.cn 中下载

【实验内容及步骤】

内容要求：



以上为实验拓扑图参考，合理规划整个网络的 IP、VLAN、静态路由，为交换机管理接口 VLAN1、路由器物理接口分配合理的 IP 地址， 其中路由器 R1 采用单臂路由方式实现区域 1 的多 VLAN 之间

通信，以及与其它区域的设备通信；路由器 R2 的一个接口连接了服务器 Server0，该服务器的 web 服务供区域 1 和区域 2 的 PC 主机访问；区域 2 的无线路由器的 LAN 口语与路由器 R3 连接;区域 2 中 Laptop0 和 PC0 与 路由器的 R3 的 F0/0 同属于一个 LAN 子网，需要将无线路由器的 DHCP 服务功能关闭。最后 通过路由器 R1、R2、R3 完成网络互联互通，

第一部分实验内容（静态路由配置）

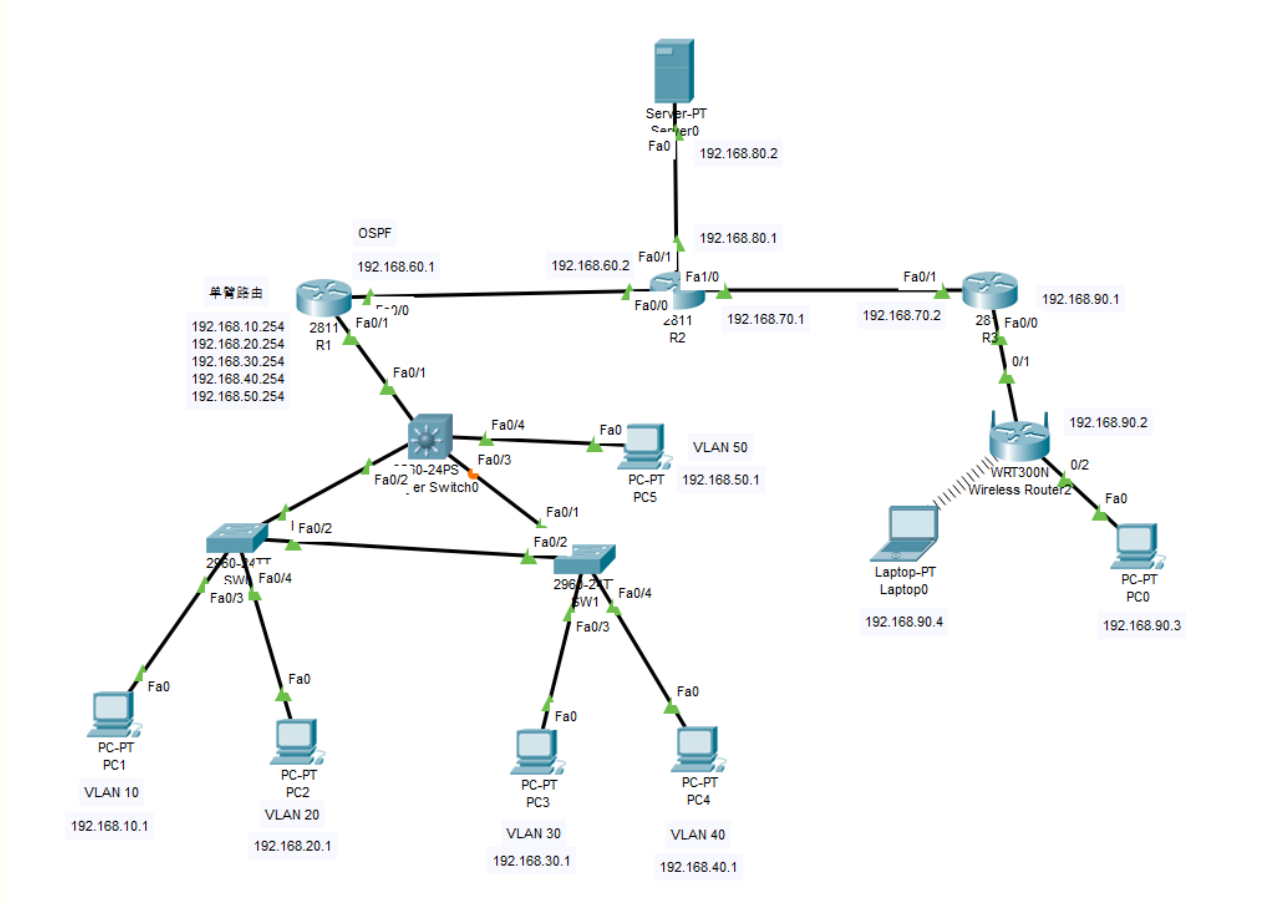
第二部分实验内容（RIP 动态路由配置）

第三部分实验内容（OSPF 动态路由配置）

1. 方案设计说明

如下图所示，区域一使用五台主机和三台交换机组成，将五台主机划分为 5 个 VLAN，分配 IP 地址 192.168.10.1 到 192.168.50.1，使用单臂路由与路由器相连；区域二为服务器，IP 地址 192.168.80.2；区域三为无线路由器和两台主机构成，IP 地址为 192.168.90.2 到 192.168.90.4.

2. 模拟实验拓扑图



3. 模拟实验操作主要过程

第一，打开软件，进入操作主界面，进行布局拓扑图

第二，规划 IP 地址或 VLAN 地址

局域网 1：192.168.10.0/24 网段

PC1 IP 192.168.10.1， 子网掩码 255.255.255.0， 网关 192.168.10.254

局域网 2：192.168.20.0/24 网段

PC2 IP 192.168.20.1， 子网掩码 255.255.255.0， 网关 192.168.20.254

局域网 3：192.168.30.0/24 网段
PC3 IP 192.168.30.1， 子网掩码 255.255.255.0， 网关 192.168.30.254

局域网 4：192.168.40.0/24 网段
PC4 IP 192.168.40.1， 子网掩码 255.255.255.0， 网关 192.168.40.254

局域网 5：192.168.50.0/24 网段
PC5 IP 192.168.50.1， 子网掩码 255.255.255.0， 网关 192.168.50.254

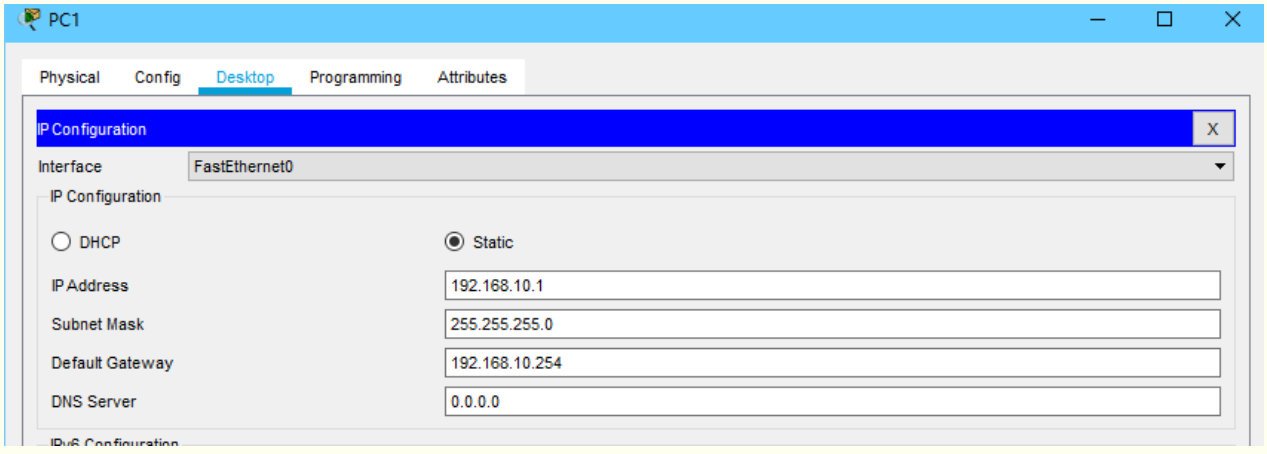
局域网 6：192.168.60.0/24 网段
网关 192.168.60.1
网关 192.168.60.2

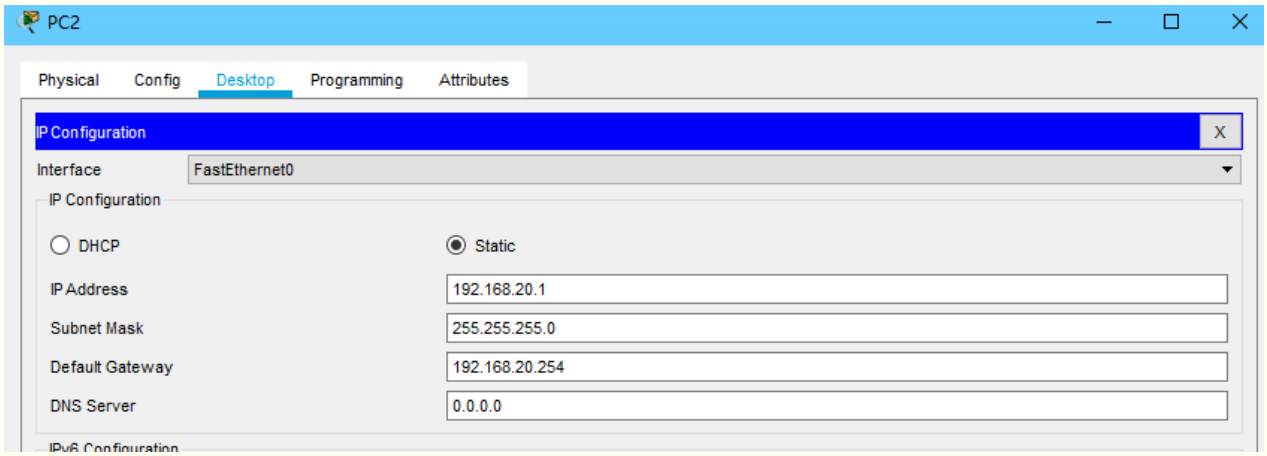
局域网 7：192.168.70.0/24 网段
网关 192.168.70.1
网关 192.168.70.2

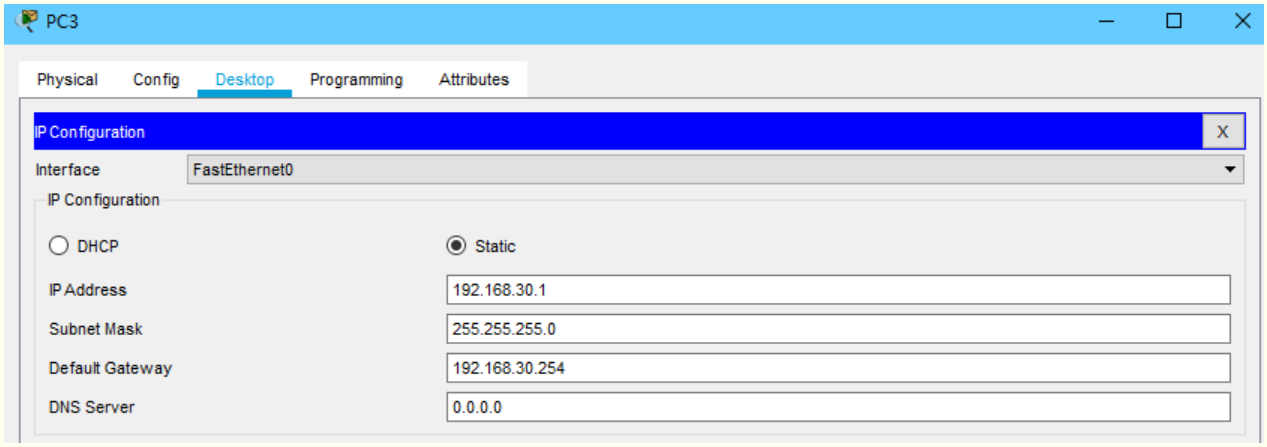
局域网 8：192.168.80.0/24 网段
Server IP 192.168.80.2， 子网掩码 255.255.255.0， 网关 192.168.80.1

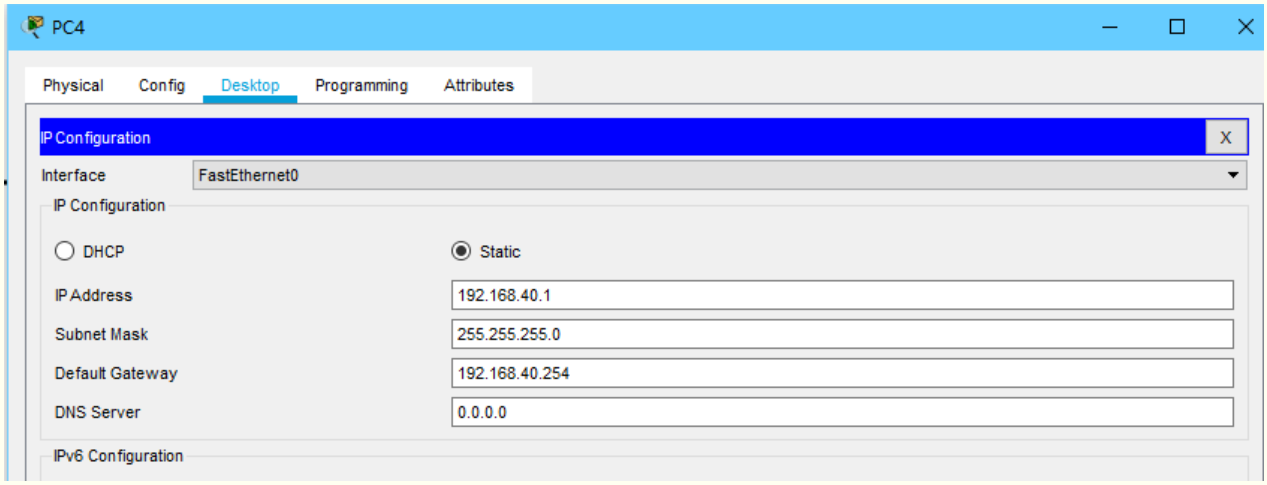
局域网 9：192.168.90.0/24 网段
PC0 IP 192.168.90.3， 子网掩码 255.255.255.0， 网关 192.168.90.1
Laptop0 IP 192.168.90.4， 子网掩码 255.255.255.0， 网关 192.168.90.1

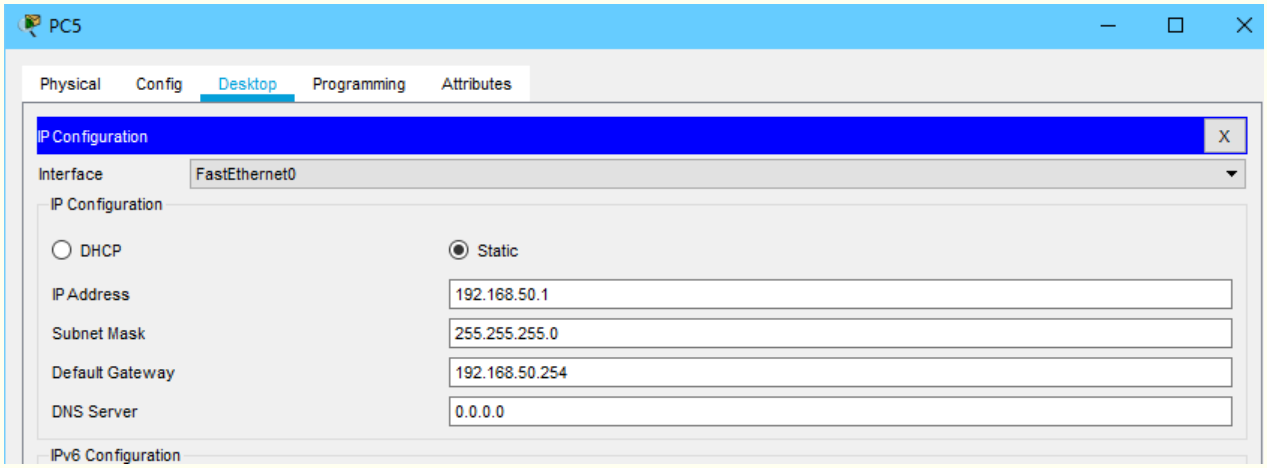
第三，通过窗口配置各个 PC 主机的 IP 地址，方法如下图所示。

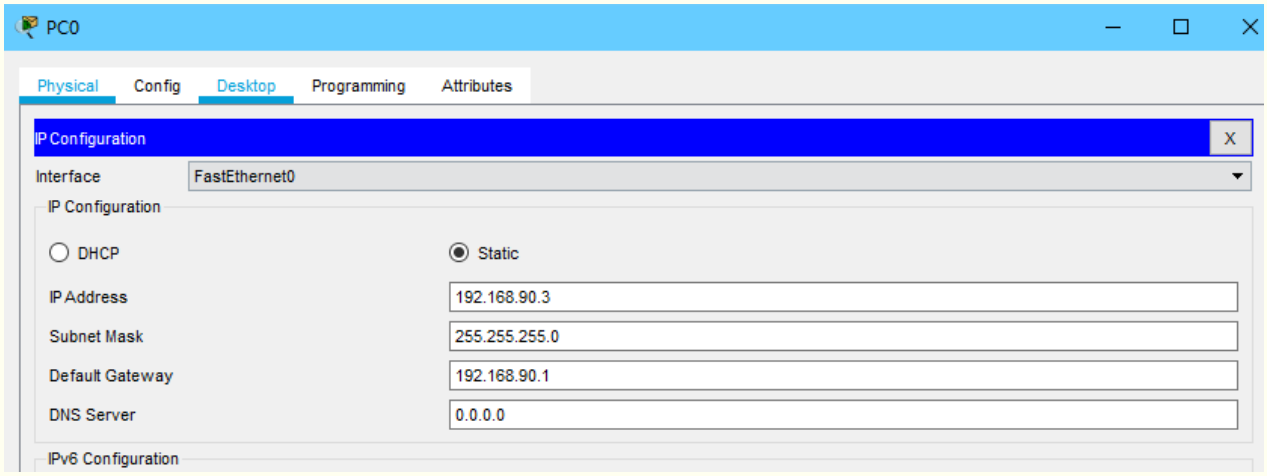


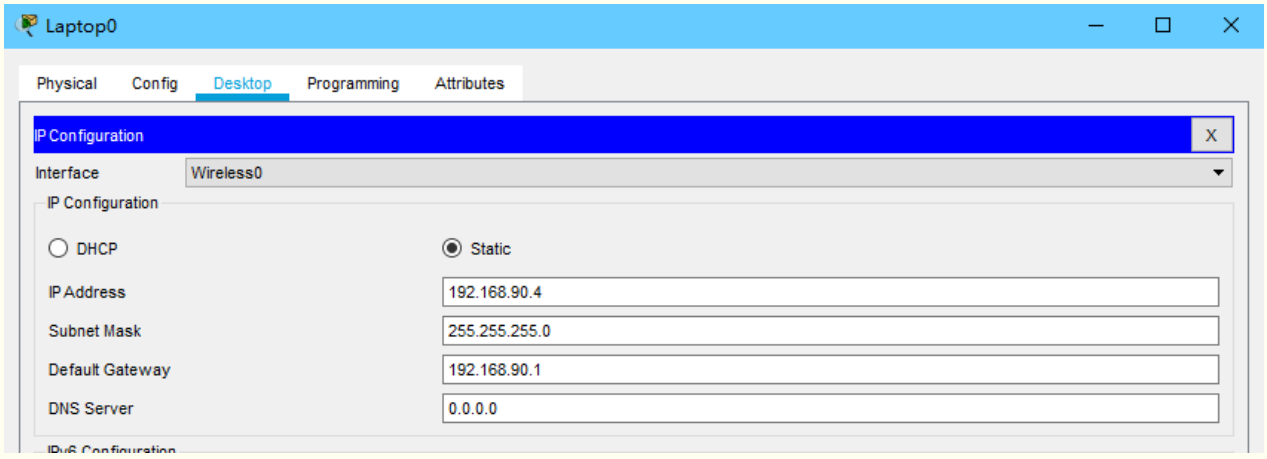

PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.20.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.20.254
DNS Server
0.0.0.0

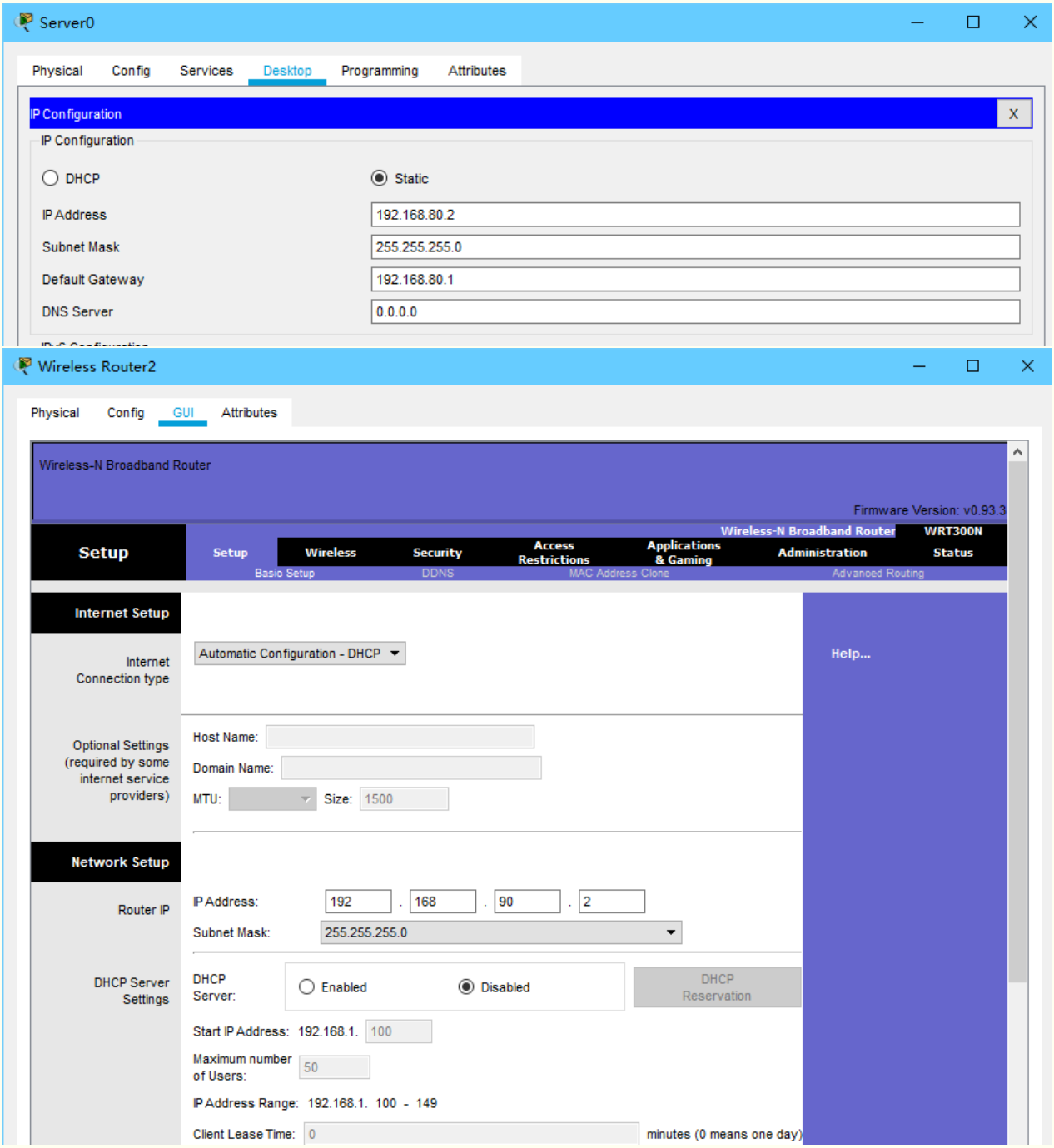

PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.30.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.30.254
DNS Server
0.0.0.0


PC4
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.40.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.40.254
DNS Server
0.0.0.0
IPv6 Configuration


PC5
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.50.1
Subnet Mask
255.255.255.0
Default Gateway
192.168.50.254
DNS Server
0.0.0.0
IPv6 Configuration


PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.90.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.90.1
DNS Server
0.0.0.0
IPv6 Configuration


Laptop0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
Wireless0
IP Configuration
DHCP
Static
IP Address
192.168.90.4
Subnet Mask
255.255.255.0
Default Gateway
192.168.90.1
DNS Server
0.0.0.0



第四，配置交换机 SW0 的内容如下：

创建 vlan 并将 Fa0/3 规划到 vlan 10，将 Fa0/4 规划到 vlan 20，将 Fa0/1、Fa0/2 接口设置为 trunk 模式

```
SW0#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
SW0(config)#vlan 10
SW0(config-vlan)#vlan 20
SW0(config-vlan)#int fa0/3
SW0(config-if)#sw
SW0(config-if)#switchport mo
SW0(config-if)#switchport mode a
SW0(config-if)#switchport mode access
SW0(config-if)#sw
SW0(config-if)#switchport a
SW0(config-if)#switchport access vlan 10
SW0(config-if)#int fa0/4
SW0(config-if)#sw mode acc
SW0(config-if)#sw acc vlan 20
SW0(config-if)#int fa0/1
SW0(config-if)#sw mode trunk
SW0(config-if)#int fa0/2
SW0(config-if)#sw mode trunk
SW0(config-if)#
```

具体指令含义见实验一。

配置交换机 SW1 的内容如下：
创建 vlan 并将 Fa0/3 规划到 vlan 30，将 Fa0/4 规划到 vlan 40，将 Fa0/1、Fa0/2 接口设置为 trunk 模式
具体指令与 SW0 类似。

配置交换机 Multilayer Switch0 的内容如下：
创建 vlan 并将 Fa0/4 规划到 vlan 50，将 Fa0/1、Fa0/2、Fa0/3 接口设置为 trunk 模式
具体指令与 SW0 类似。

配置路由器 R1 的内容如下：
对接口 Fa0/1 配置单臂路由：

int f0/1.1	选择子接口 1
encapsulation dot1Q 10	将接口分配给 vlan 10
ip add 192.168.10.254 255.255.255.0	给接口分配网关 192.168.10.254/24

```
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int f0/1.1
Router(config-subif)#en
Router(config-subif)#encapsulation do
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip add 192.168.10.254 255.255.255.0
Router(config-subif)#
```

对其余子接口类似配置
最后将接口 Fa0/1 打开

```
Router(config)#int fa0/1
Router(config-if)#no sh
Router(config-if)#no shutdown
Router(config-if)#
```

对接口 Fa0/0 配置网关 192.168.60.1/24 并打开：

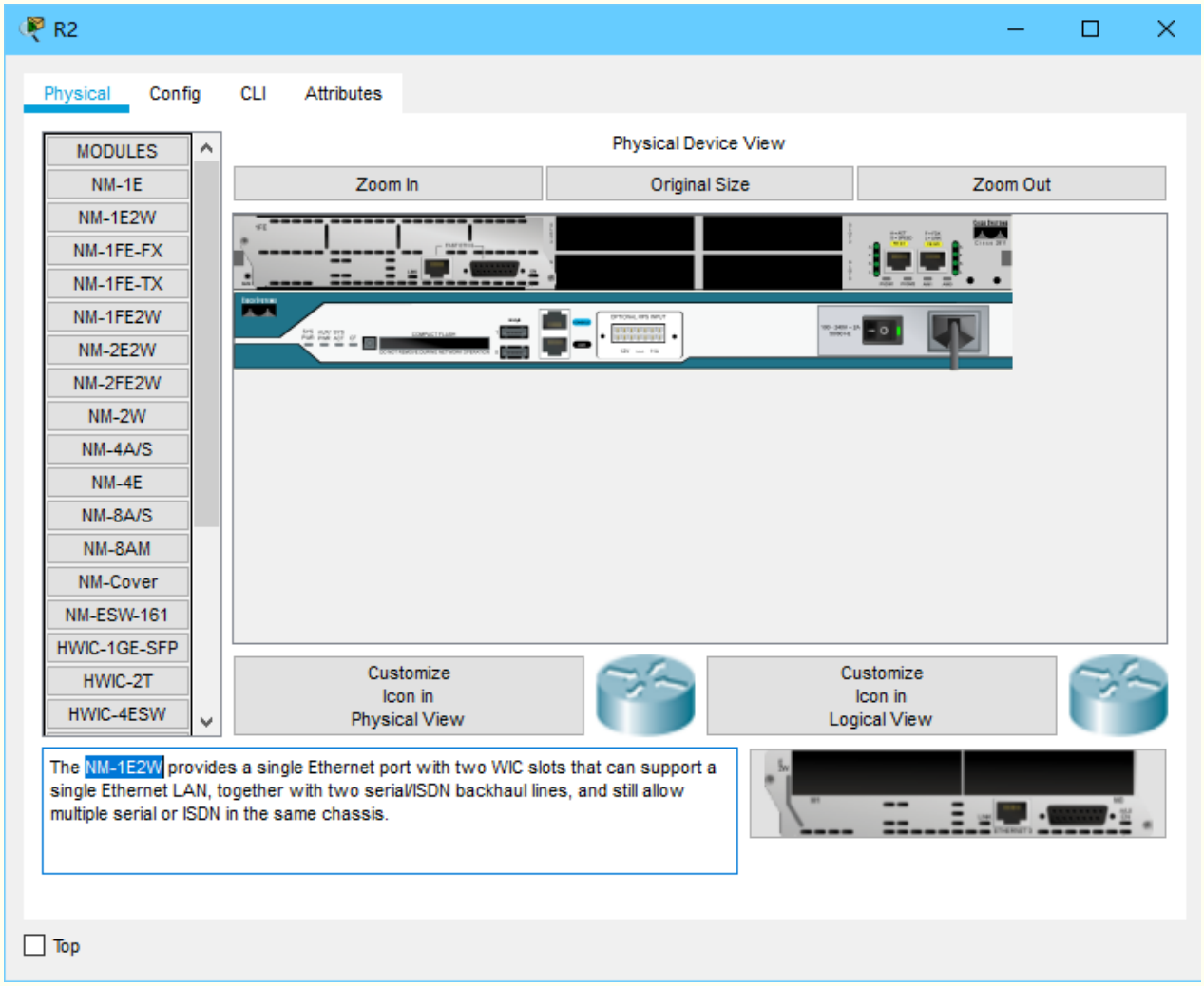
int f0/0 选择接口

ip add 192.168.60.1 255.255.255.0 给接口分配网关 192.168.60.1/24

no shutdown 打开接口

```
Router(config)#int fa0/0
Router(config-if)#ip add 192.168.60.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#no shutdown
Router(config-if)#
```

配置路由器 R2 的内容如下：
提前添加模块 NM-1E2W 以增加接口数量



对接口 Fa0/0 配置网关 192.168.60.2/24 并打开
对接口 Fa1/0 配置网关 192.168.70.1/24 并打开
对接口 Fa0/1 配置网关 192.168.80.1/24 并打开
具体命令与路由器 R1 的 Fa0/0 接口配置类似。

配置路由器 R3 的内容如下：
对接口 Fa0/1 配置网关 192.168.70.2/24 并打开
对接口 Fa0/0 配置网关 192.168.90.1/24 并打开
具体命令与路由器 R1 的 Fa0/0 接口配置类似。

RIP 动态路由配置：
配置路由器 R1 的内容如下：
选择协议 RIP，将路由器直接连接的网络全部添加到 RIP 协议中：

route rip	选择路由协议 RIP
network 192.168.10.0	添加网络 192.168.10.0/24
network 192.168.20.0	添加网络 192.168.20.0/24

重复直到将全部网络添加完成。

```
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#route rip
Router(config-router)#network 192.168.10.0
Router(config-router)#network 192.168.20.0
Router(config-router)#network 192.168.30.0
Router(config-router)#
```

其他 RIP 配置：

distance 80	设置 RIP 管理距离
version 2	设置 RIP 版本

```
Router(config)#route rip
Router(config-router)#
Router(config-router)#distance 80
Router(config-router)#ver
Router(config-router)#version 2
Router(config-router)#version 1
Router(config-router)#
```

配置路由器 R2 的内容如下：
将以下路由器直接连接的网络添加到 RIP 协议中：

network 192.168.60.0

network 192.168.70.0

network 192.168.80.0

具体命令与路由器 R1 的 RIP 配置类似。

配置路由器 R3 的内容如下：
将以下路由器直接连接的网络添加到 RIP 协议中：

network 192.168.70.0

network 192.168.90.0

具体命令与路由器 R1 的 RIP 配置类似。

检查路由表：
R1：

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, FastEthernet0/1.1
C    192.168.20.0/24 is directly connected, FastEthernet0/1.2
C    192.168.30.0/24 is directly connected, FastEthernet0/1.3
C    192.168.40.0/24 is directly connected, FastEthernet0/1.4
C    192.168.50.0/24 is directly connected, FastEthernet0/1.5
C    192.168.60.0/24 is directly connected, FastEthernet0/0
R    192.168.70.0/24 [80/1] via 192.168.60.2, 00:00:11, FastEthernet0/0
R    192.168.80.0/24 [80/1] via 192.168.60.2, 00:00:11, FastEthernet0/0
R    192.168.90.0/24 [80/2] via 192.168.60.2, 00:00:11, FastEthernet0/0
C    192.168.170.0/24 is directly connected, FastEthernet0/1.7
```

R2：

```
R    192.168.10.0/24 [120/1] via 192.168.60.1, 00:00:04, FastEthernet0/0
R    192.168.20.0/24 [120/1] via 192.168.60.1, 00:00:04, FastEthernet0/0
R    192.168.30.0/24 [120/1] via 192.168.60.1, 00:00:04, FastEthernet0/0
R    192.168.40.0/24 [120/1] via 192.168.60.1, 00:00:04, FastEthernet0/0
R    192.168.50.0/24 [120/1] via 192.168.60.1, 00:00:04, FastEthernet0/0
C    192.168.60.0/24 is directly connected, FastEthernet0/0
C    192.168.70.0/24 is directly connected, FastEthernet1/0
C    192.168.80.0/24 is directly connected, FastEthernet0/1
R    192.168.90.0/24 [120/1] via 192.168.70.2, 00:00:03, FastEthernet1/0
```

R3：

```
R    192.168.10.0/24 [50/2] via 192.168.70.1, 00:00:26, FastEthernet0/1
R    192.168.20.0/24 [50/2] via 192.168.70.1, 00:00:26, FastEthernet0/1
R    192.168.30.0/24 [50/2] via 192.168.70.1, 00:00:26, FastEthernet0/1
R    192.168.40.0/24 [50/2] via 192.168.70.1, 00:00:26, FastEthernet0/1
R    192.168.50.0/24 [50/2] via 192.168.70.1, 00:00:26, FastEthernet0/1
R    192.168.60.0/24 [50/1] via 192.168.70.1, 00:00:26, FastEthernet0/1
C    192.168.70.0/24 is directly connected, FastEthernet0/1
R    192.168.80.0/24 [50/1] via 192.168.70.1, 00:00:26, FastEthernet0/1
C    192.168.90.0/24 is directly connected, FastEthernet0/0
```

说明 RIP 配置成功。

OSPF 动态路由配置：

配置路由器 R1 的内容如下：

选择协议 OSPF，将路由器直接连接的网络全部添加到 OSPF 协议中：

route ospf 1　　选择路由协议 OSPF 进程 1

network 192.168.10.0 0.0.0.255 area 0　　添加网络 192.168.10.0/24 到区域 0

network 192.168.20.0 0.0.0.255 area 0　　添加网络 192.168.20.0/24 到区域 0

重复直到将全部网络添加完成。

```
Router(config)#route ospf 1
Router(config-router)#network 192.168.10.0 0.0.0.255 area 0
Router(config-router)#network 192.168.20.0 0.0.0.255 area 0
Router(config-router)#network 192.168.30.0 0.0.0.255 area 0
Router(config-router)#
```

配置路由器 R2 的内容如下：

将以下路由器直接连接的网络添加到 OSPF 协议进程 1 区域 0 中：

network 192.168.60.0 0.0.0.255 area 0

network 192.168.70.0 0.0.0.255 area 0

network 192.168.80.0 0.0.0.255 area 0

具体命令与路由器 R1 的 OSPF 配置类似。

配置路由器 R3 的内容如下：

将以下路由器直接连接的网络添加到 OSPF 协议进程 1 区域 0 中：

network 192.168.70.0 0.0.0.255 area 0

network 192.168.90.0 0.0.0.255 area 0

具体命令与路由器 R1 的 OSPF 配置类似。

检查路由表

R1：

```
C    192.168.10.0/24 is directly connected, FastEthernet0/1.1
C    192.168.20.0/24 is directly connected, FastEthernet0/1.2
C    192.168.30.0/24 is directly connected, FastEthernet0/1.3
C    192.168.40.0/24 is directly connected, FastEthernet0/1.4
C    192.168.50.0/24 is directly connected, FastEthernet0/1.5
C    192.168.60.0/24 is directly connected, FastEthernet0/0
O    192.168.70.0/24 [110/2] via 192.168.60.2, 00:39:12, FastEthernet0/0
O    192.168.80.0/24 [110/2] via 192.168.60.2, 00:39:12, FastEthernet0/0
O    192.168.90.0/24 [110/3] via 192.168.60.2, 00:39:02, FastEthernet0/0
```

R2：

```
O    192.168.10.0/24 [110/2] via 192.168.60.1, 00:39:43, FastEthernet0/0
O    192.168.20.0/24 [110/2] via 192.168.60.1, 00:39:43, FastEthernet0/0
O    192.168.30.0/24 [110/2] via 192.168.60.1, 00:39:43, FastEthernet0/0
O    192.168.40.0/24 [110/2] via 192.168.60.1, 00:39:43, FastEthernet0/0
O    192.168.50.0/24 [110/2] via 192.168.60.1, 00:39:43, FastEthernet0/0
C    192.168.60.0/24 is directly connected, FastEthernet0/0
C    192.168.70.0/24 is directly connected, FastEthernet1/0
C    192.168.80.0/24 is directly connected, FastEthernet0/1
O    192.168.90.0/24 [110/2] via 192.168.70.2, 00:39:43, FastEthernet1/0
```

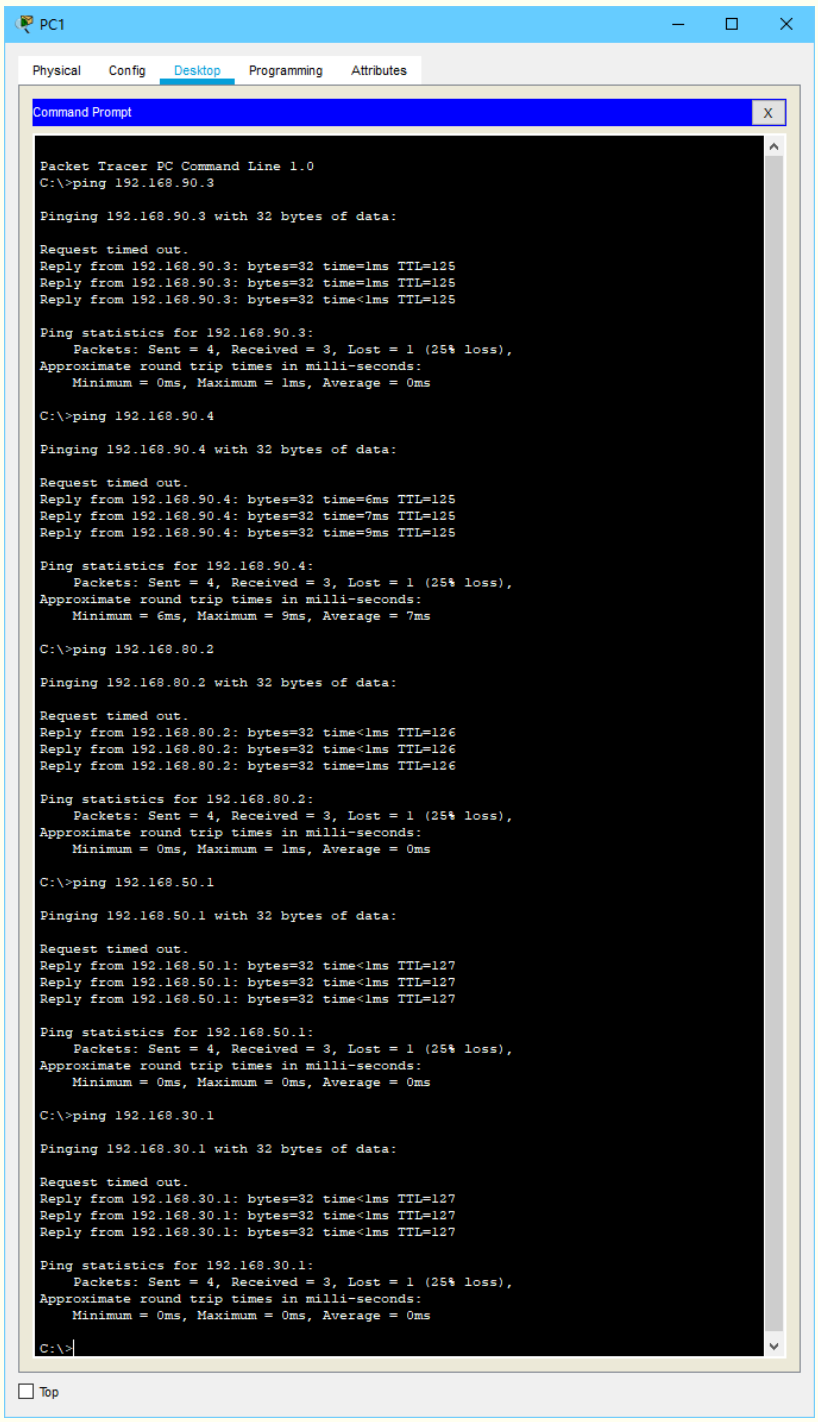
R3：

```
O    192.168.10.0/24 [110/3] via 192.168.70.1, 00:39:56, FastEthernet0/1
O    192.168.20.0/24 [110/3] via 192.168.70.1, 00:39:56, FastEthernet0/1
O    192.168.30.0/24 [110/3] via 192.168.70.1, 00:39:56, FastEthernet0/1
O    192.168.40.0/24 [110/3] via 192.168.70.1, 00:39:56, FastEthernet0/1
O    192.168.50.0/24 [110/3] via 192.168.70.1, 00:39:56, FastEthernet0/1
O    192.168.60.0/24 [110/2] via 192.168.70.1, 00:39:56, FastEthernet0/1
C    192.168.70.0/24 is directly connected, FastEthernet0/1
O    192.168.80.0/24 [110/2] via 192.168.70.1, 00:39:56, FastEthernet0/1
C    192.168.90.0/24 is directly connected, FastEthernet0/0
```

说明 OSPF 配置成功。

第五，验证配置结果

在 PC1 中启动 CMD 窗口，通过 ping 来验证，结果如下图



说明 PC1 可以与区域 2、区域 3 互连互通。

在其余设备中启动 CMD 窗口，通过 ping 来验证，结果类似，均可以互连互通。

在交换机 SW0 中，通过命令 show vlan 查看 vlan 配置验证是否生效

```
SW0#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   VLAN0010                         active    Fa0/3
20   VLAN0020                         active    Fa0/4
30   VLAN0030                         active
40   VLAN0040                         active
50   VLAN0050                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

交换机 SW1，Multilayer Switch0 结果类似。

9 访问控制列表 ACL

9.1 访问控制列表

78. 访问控制列表（Access Control List）

是一个有序的语句集，它通过对比报文中字段值与访问控制列表参数，来允许或拒绝报文通过某个接口。

79. 访问控制列表作用

安全控制
流量过滤
数据流量标识

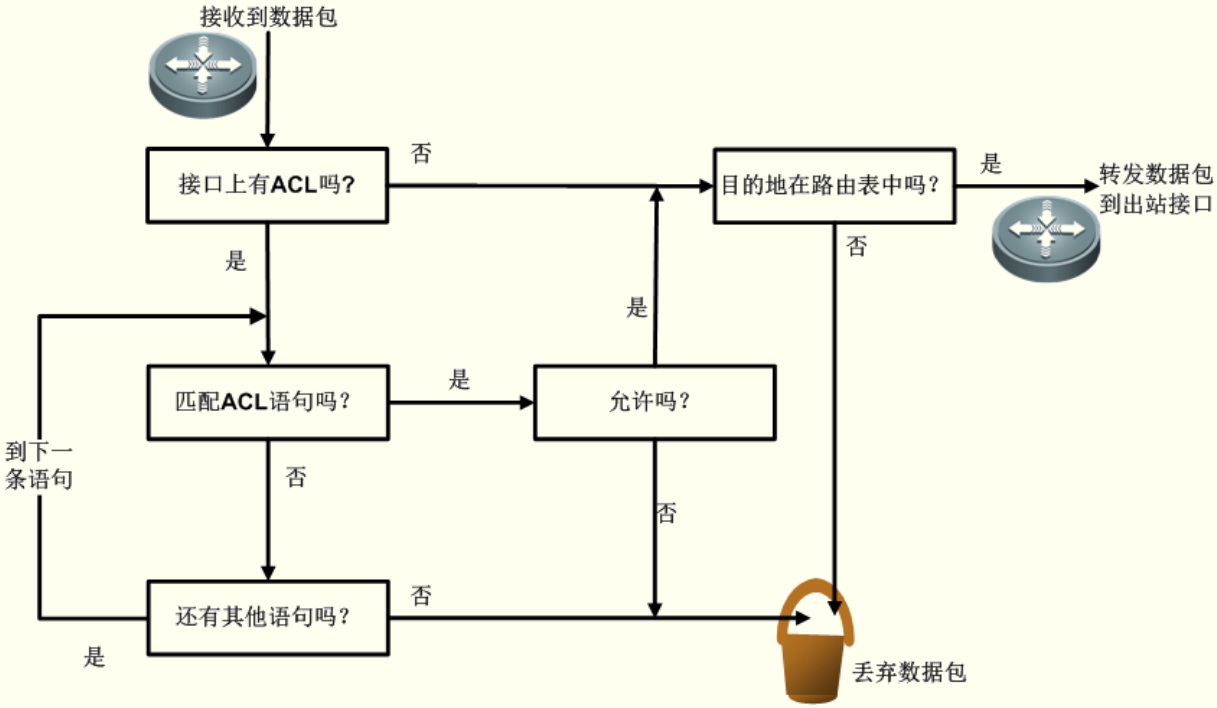
80. ACL 语句组成

条件：用来匹配数据包中字段值
操作：条件匹配时，可以采取允许和拒绝两个操作

81. ACL 工作原理

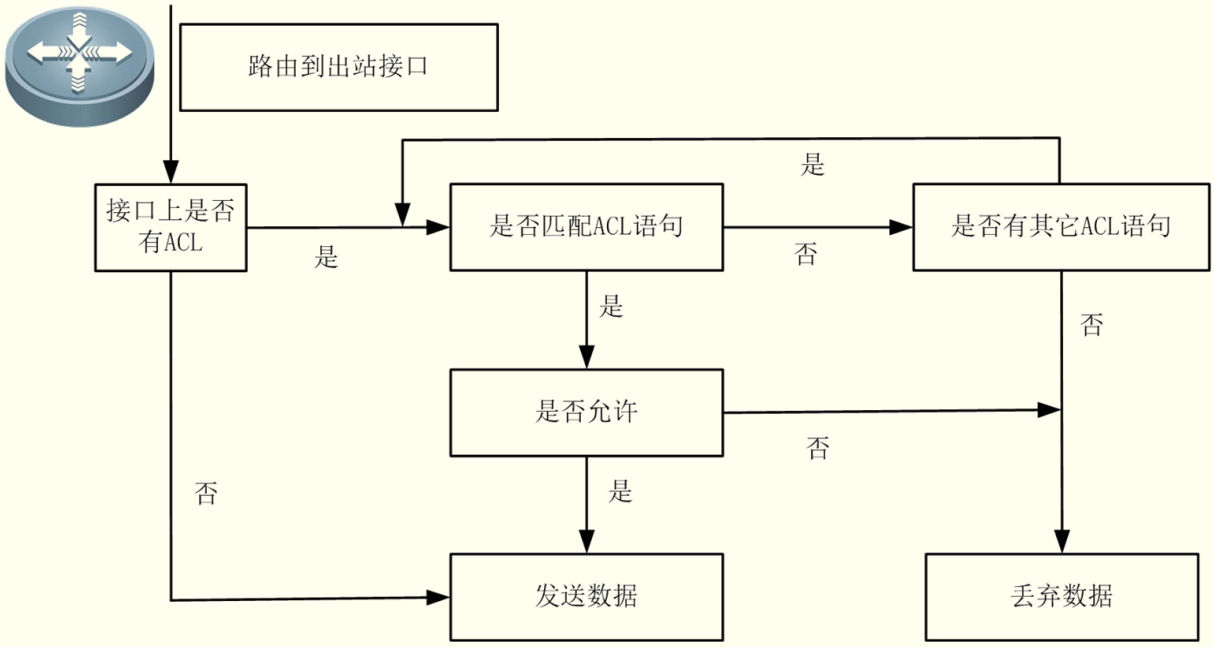
(1) 入站 ACL

入站数据先判断 ACL 后执行路由



(2) 出站 ACL

出站数据先进行路由再应用 ACL



82. ACL 基本规则

- ACL 规则按名称或编号进行分组
- 列表中每条 ACL 语句有一组条件和一个操作，如果需要多个条件或多个操作，则必须使用多个 ACL 语句来完成
- 如果当前语句的条件没有匹配，则处理列表中的下一条语句
- 如果条件匹配，则执行语句后面的操作，且不再与其他 ACL 语句进行匹配
- 如果列表中的所有语句都不匹配，那么丢弃该数据包

注意：

- 由于 ACL 语句**默认是拒绝不匹配的数据包**，所以在列表中至少要有一个允许的操作。否则，所有数据包都会被拒绝掉
- 注意语句的顺序。条件严的语句应该放在列表的顶部，条件宽的语句应该放在列表的底部。从而，避免条件严的语句永远也得不到执行

83. 注意事项

- 一个 ACL 列表中至少要有一条允许或拒绝的语句
- 只能在设备的每个接口、每个协议、每个方向上应用一个 ACL
- ACL 只能应用在接口上
- 先处理入站 ACL，再进行数据路由
- 先进行数据路由，再处理出站接口上的出站 ACL
- ACL 会影响通过接口的流量和速度，但不会过滤路由器本身产生的流量

84. 放置位置

- 只过滤数据包**源地址**的 ACL 应该放置在**离目的地尽量近的地方**
- 过滤数据包的源地址和目的地址以及其他信息的 ACL，则应该尽量放在离源地址近的地方

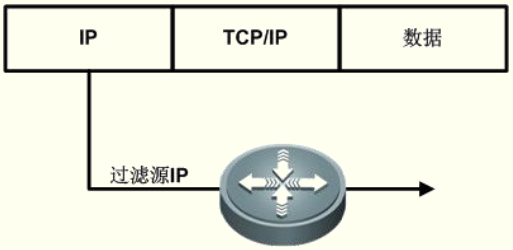
9.2 ★配置访问控制列表

85. 标准和扩展 ACL P195

标准 ACL：只能过滤 IP 数据包头中的源 IP 地址
扩展 ACL：可以过滤源 IP 地址、目的 IP 地址、协议（TCP/IP）、协议信息（端口号、标志代码）等
时间 ACL：可以根据时间段进行扩展 ACL 过滤
专家 ACL：可以过滤源 IP、源 MAC、源端口、目标 IP、目标 MAC、目标端口、时间等

86. 标准 ACL

标准 ACL 只能过滤 IP 数据包头中的源 IP 地址



标准 ACL 通常配置在路由器上实现以下功能：

- 限制通过 VTY 线路对路由器的访问（telnet、SSH）
- 限制通过 HTTP 或 HTTPS 对路由器的访问
- 过滤路由更新

87. 创建标准 ACL P196

(1) 使用编号创建

创建 ACL
(config)#access-list *listnumber* { permit | deny } *address* [*wildcard–mask*]

在接口上应用
(config-if)#ip access-group *{id|name}*{in|out}
In：当数据流入路由器接口时
Out：当数据流出路由器接口时

(2) 使用命名创建

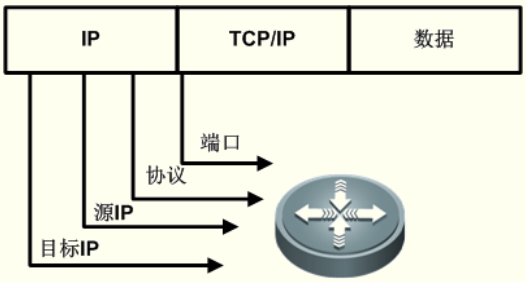
定义 ACL 名称
(config)#ip access-list standard name

定义规则
(config-std-nacl)#deny|permit [source wildcard any]

在接口上应用

88. 扩展 ACL

扩展的 IP 访问表用于扩展报文过滤的能力。



扩展访问列表允许过滤内容:
源和目的地址、协议、源和目的端口以及在特定报文字段中允许进行特殊位比较的各种选项。

89. 创建扩展 ACL P199

(1) 使用编号创建

创建 ACL
(config)#access-list listnumber { permit | deny } protocol source source- wildcard–mask destination destination-wildcard–mask [operator operand]

在接口上应用
(config-if)#ip access-group {id|name} {in|out}

(2) 使用命名创建

定义 ACL 名称
(config)#ip access-list extended name

定义规则
(config-ext-nacl)#{deny|permit} protocol {source source-wildcard |host source| any}[operator port]

在接口上应用

10 网络地址转换 NAT

10.1 网络地址转换 NAT

90. 网络地址转换 NAT P205

(1) 动态 NAT

使用公有地址池，并以先到先得的原则分配这些地址。当具有私有 IP 地址的主机请求访问 Internet 时，动态 NAT 从地址池中选择一个未被其它主机占用的 IP 地址。这就是到目前为止所介绍的映射。

(2) 静态 NAT

使用本地地址与全局地址的一对一映射，这些映射保持不变。静态 NAT 对于必须具有一致的地址、可从 Internet 访问的 Web 服务器或主机特别有用。这些内部主机可能是企业服务器或网络设备。

(3) NAT 过载（有时称为端口地址转换或 PAT）

将多个私有 IP 地址映射到一个或少数几个公有 IP 地址。因为每个私有地址也会用端口号加以跟踪。大多数家用路由器就是这样工作的。

91. ★配置静态 NAT P209

步骤	操作	备注
1	建立内部本地地址与内部全局地址之间的静态转换。Router(config)#**ip nat inside source static** *local-ip global-ip*	输入全局命令 **no ip nat inside source static** 可删除静态源地址转换。
2	指定内部接口。Router(config)#**interface** *type number*	输入 **interface** 命令。CLI 提示符从 (config)# 变为 (config-if)#
3	将该接口标记为与内部连接。Router(config-if)#**ip nat inside**	
4	退出接口配置模式。Router(config-if)# **exit**	
5	指定外部接口。Router(config)#**interface** *type number*	
6	将该接口标记为与外部连接。Router(config-if)#**ip nat outside**	

92. ★配置动态 NAT P209

步骤	操作	备注
1	根据需要定义待分配的全局地址池。Router(config)#**ip nat pool name** *start-ip end-ip* { **netmask** *netmask*|**prefix-length** *prefix-length*}	输入全局命令 **no ip nat pool** *name* 以删除全局地址池。
2	定义一个标准访问列表，以允许待转换的地址通过。 Router(config)#**access-list** access-list-number **permit** source [source-wildcard]	输入全局命令 **no access-list** *access-list-number* 可删除访问列表。
3	建立动态源地址转换，指定上一步骤中定义的访问列表。 Router(config)#**ip nat inside source list** *access-list-number* **pool** *name*	输入全局命令 **no ip nat inside source** 可删除动态源地址转换。
4	指定内部接口。Router(config)#**interface** *type number*	输入 **interface** 命令。CLI 提示符从 (config)# 变为 (config-if)#。
5	将该接口标记为与内部连接。Router(config-if)#**ip nat inside**	
6	指定外部接口。Router(config)#**interface** *type number*	
7	将该接口标记为与外部连接。Router(config-if)#**ip nat outside**	
8	退出接口配置模式。 Router(config-if)# **exit**	

93. ★配置 NAT 过载（PAT） P211

(1)

步骤	操作	备注
1	定义一个标准访问列表，以允许待转换的地址通过。 Router(config)#**access-list** *acl-number* **permit** *source [source-wildcard]*	输入全局命令 **no access-list** *access-list-number* 可删除访问列表。
2	建立动态源地址转换，指定上一步骤中定义的访问列表。 Router(config)#**ip nat inside source list** *acl-number* **interface** *interface* **overload**	输入全局命令 **no ip nat inside source** 可删除动态源地址转换。overload 关键字会启用 PAT。
3	指定内部接口。 Router(config)#**interface** *type number* Router(config-if)#**ip nat inside**	输入 **interface** 命令。CLI 提示符从 (config)# 变为 (config-if)#
4	指定外部接口。 Router(config-if)#**interface** *type number* Router(config-if)#**ip nat outside**	

(2)

步骤	操作	备注
1	定义一个标准访问列表，以允许待转换的地址通过。 Router(config)#**access-list** *acl-number* **permit** *source [source-wildcard]*	输入全局命令 **no access-list** *access-list-number* 可删除访问列表。
2	指定要用于过载的全局地址池。 Router(config)#**ip nat pool** *name start-ip end-ip* {**netmask** *netmask* | **prefix-length** *prefix-length*}	
3	建立过载转换。 Router {config} #**ip nat inside source list** *acl-number* **pool** *name* **overload**	
4	指定内部接口。 Router(config)#**interface** *type number* Router(config-if)#**ip nat inside**	输入 **interface** 命令。CLI 提示符从 (config)# 变为 (config-if)#
5	指定外部接口。 Router(config-if)#**interface** *type number* Router(config-if)#**ip nat outside**	

94. 检验 NAT 和 NAT 过载

步骤 1. 根据配置，清楚地确定应该实现什么样的 NAT。这可能会揭示出配置问题。

步骤 2. 使用 **show ip nat translations** 命令检验转换表中转换条目是否正确。

步骤 3. 使用 clear 和 debug 命令检验 NAT 是否如预期一样工作。检查动态条目被清除后，是否又被重新创建出来。

步骤 4. 详细审查数据包传送情况，确认路由器具有移动数据包所需的正确路由信息。
使用 debug ip nat 命令显示关于被路由器转换的每个数据包的信息，检验 NAT 功能的运作。

10.2 实验三 访问控制列表及 NAT 的应用

【实验目的】

1、熟练掌握 NAT 的静态 NAT、动态 NAT、PNAT（端口复用 overload）的配置。
2、熟练掌握 ACL 的标准和扩展的配置，选择合适的 ACL 与 NAT 配合完成局域网 NAT 方式访问公网。

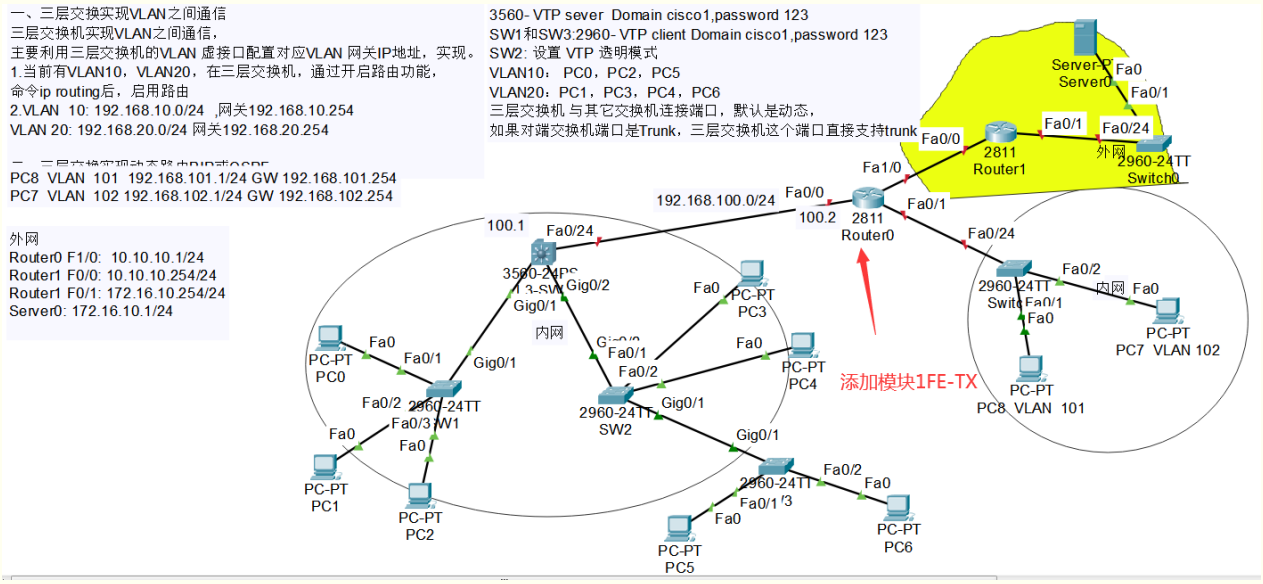
【实验环境】

Cisco PacketTracer 7.2 及以上版本模拟器软件，
下载位置：https://www.netacad.com/portal/resources/packet-tracer（需要注册下载）或者 在 jxpt.cuit.edu.cn 中下载

【实验内容及步骤】

内容要求：

在**实验 3 的拓扑图及配置的基础**上，修改 Router0 路由器，添加一个模块 1FE-TX 网口，并与服务器 Server 连接，如下图所示（根据情况，同学们也可以自行架构网络拓扑，实现 NAT 和 ACL 的各项知识点内容即可）



完成配置要求如下：

首先自行确定路由器 Router0 的 F1/0 接口地址，并将 Router0 的 F1/0 作为内网的外网出口，并自行假定 NAT Pool 地址池（与 Router0 的接口 F1/0 同一子网网络）。同时自行假定 Server0 的 IP 地址和网关（网关地址即为 路由器 Router1 的 F0/1 地址）。

要求 PC2 和 PC1 不能访问外网 80 端口，但可以访问外网其他端口，PC5、PC6 不能 ping 通 PC7，但是 PC7 可以 ping 通 PC5 和 PC6.

第一种情况配置：

路由器 Router0 的静态 NAT 配置：许可内网络的 PC1、PC2、PC8、PC7 4 台主机可以静态 NAT 后与 Server0 通信，并选择合理的 ACL 标准或扩展，

第二种情况配置：

在路由器 Router0 上采用 NAT 地址池实现动态 NAT 配置，除了主机 PC1、PC2 外，其他所有内网主机被许 NAT 访问 Server0。

第三种情况配置：

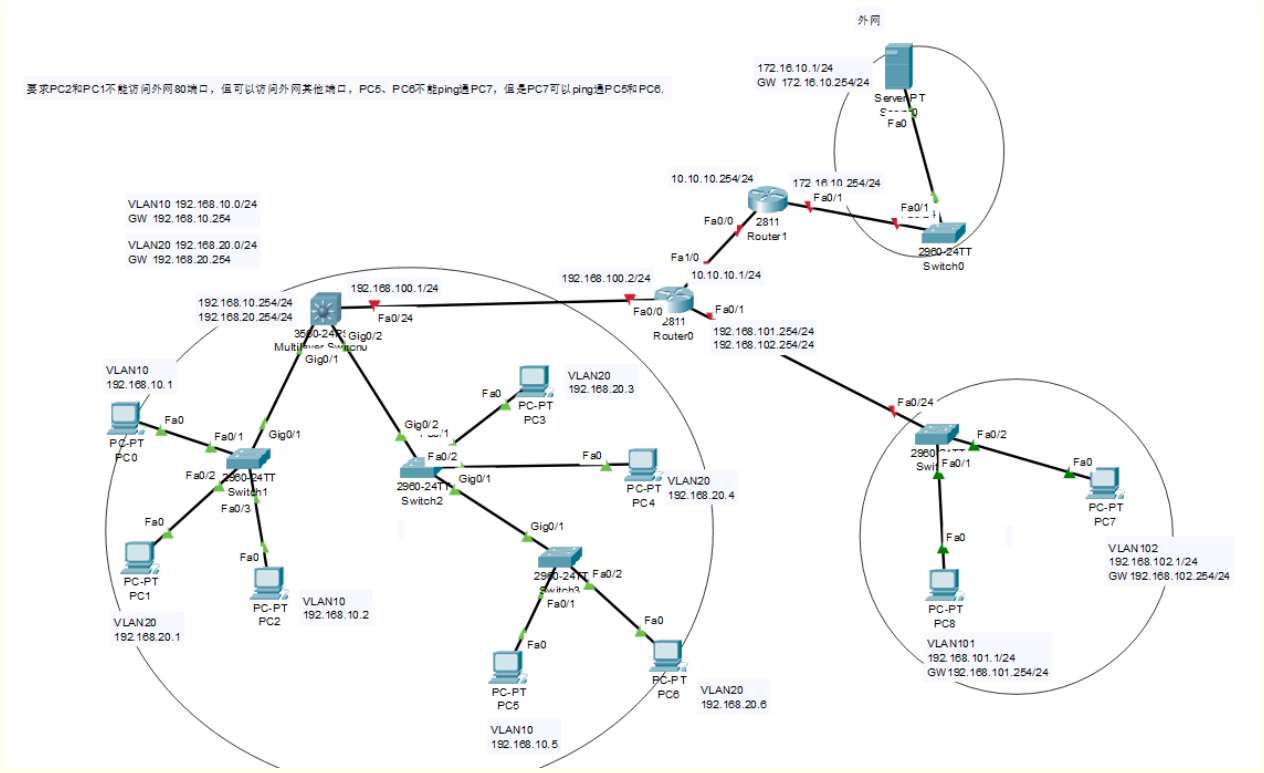
（1）采用地址池的 OverLoad 方式，在路由器 Router0 上采用 PNAT 方式实现内网可以被许可 NAT 方式访问 Server0

（2）采用路由器接口的 Overload 方式，只许可内网主机可以通过 NAT 方式访问 Server0 的 80 端口，其他不许可。

1. 方案设计说明

路由器 R0 连接了两个交换机（三层交换机和 SW4）和一个路由器 R1，其中 R1 作为外网路由器，两个交换机作为内网。内网通过路由器 R0 进行 NAT 与外网进行数据通信。三层交换机 F0/24 接口采用路由功能与 R0 相连，另外两个接口连接两个 VLAN：10 和 20。交换机 SW4 所在子网具有两个 VLAN：101 和 102，通过单臂路由与 R0 相连。

2. 模拟实验拓扑图



3. 模拟实验操作主要过程

第一，打开软件，进入操作主界面，进行布局拓扑图

第二，规划 IP 地址或 VLAN 地址

局域网 1：192.168.10.0/24 网段

PC0	IP 192.168.10.1	子网掩码 255.255.255.0	网关 192.168.10.254
PC2	IP 192.168.10.2	子网掩码 255.255.255.0	网关 192.168.10.254
PC5	IP 192.168.10.5	子网掩码 255.255.255.0	网关 192.168.10.254

局域网 2：192.168.20.0/24 网段

PC1	IP 192.168.20.1	子网掩码 255.255.255.0	网关 192.168.20.254
PC3	IP 192.168.20.3	子网掩码 255.255.255.0	网关 192.168.20.254
PC4	IP 192.168.20.4	子网掩码 255.255.255.0	网关 192.168.20.254
PC6	IP 192.168.20.6	子网掩码 255.255.255.0	网关 192.168.20.254

局域网 3：192.168.100.0/24 网段

MSW	IP 192.168.100.1	子网掩码 255.255.255.0	网关 -
R0	IP 192.168.100.2	子网掩码 255.255.255.0	网关 -

局域网 4：192.168.101.0/24 网段

PC8	IP 192.168.101.1	子网掩码 255.255.255.0	网关 192.168.101.254
R0	IP 192.168.101.254	子网掩码 255.255.255.0	网关 -

局域网 5：192.168.102.0/24 网段

PC7	IP 192.168.102.1	子网掩码 255.255.255.0	网关 192.168.102.254
R0	IP 192.168.102.254	子网掩码 255.255.255.0	网关 -

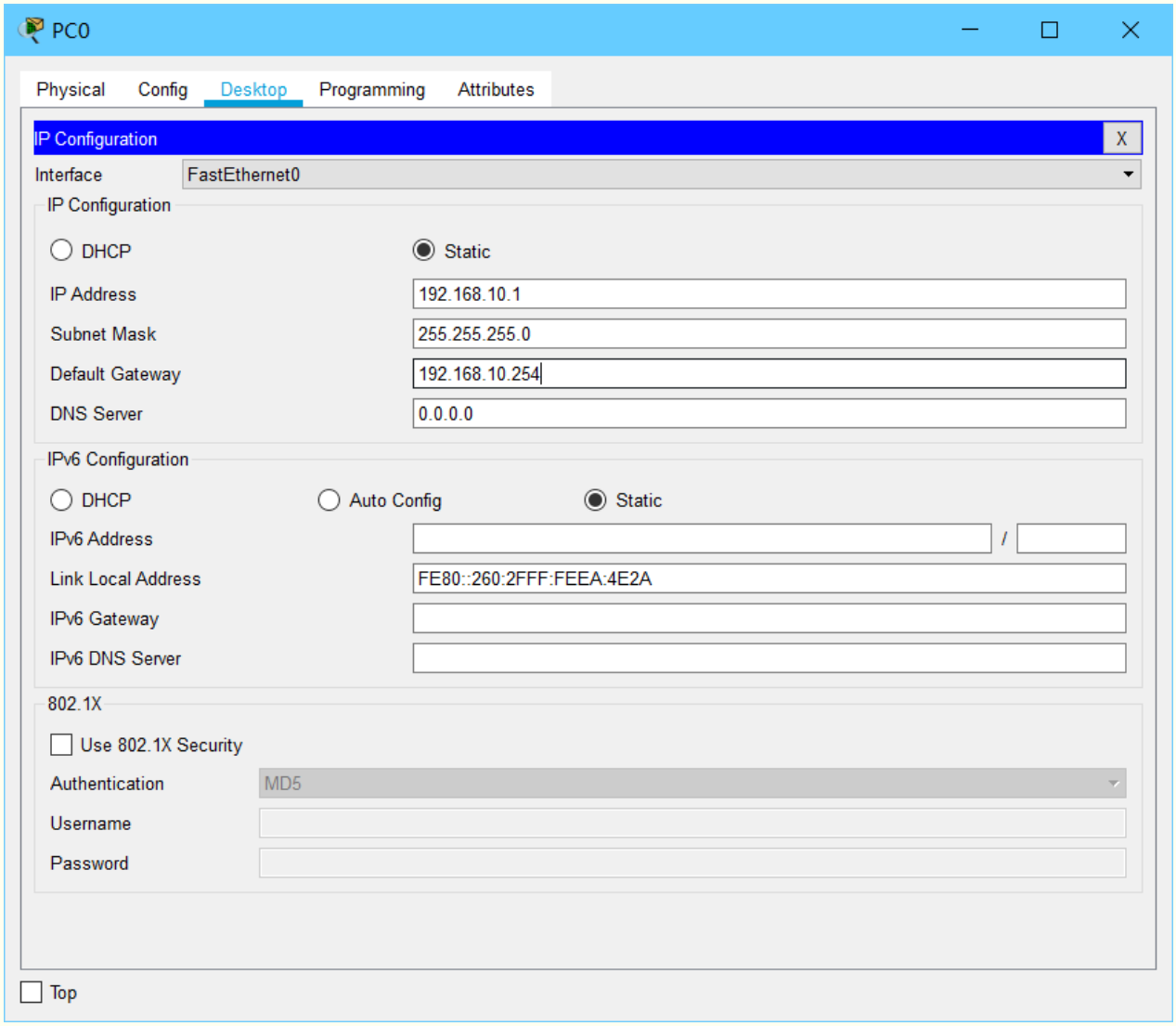
外网：10.10.10.0/24 网段

R0	IP 10.10.10.1	子网掩码 255.255.255.0	网关 -
R1	IP 10.10.10.254	子网掩码 255.255.255.0	网关 -

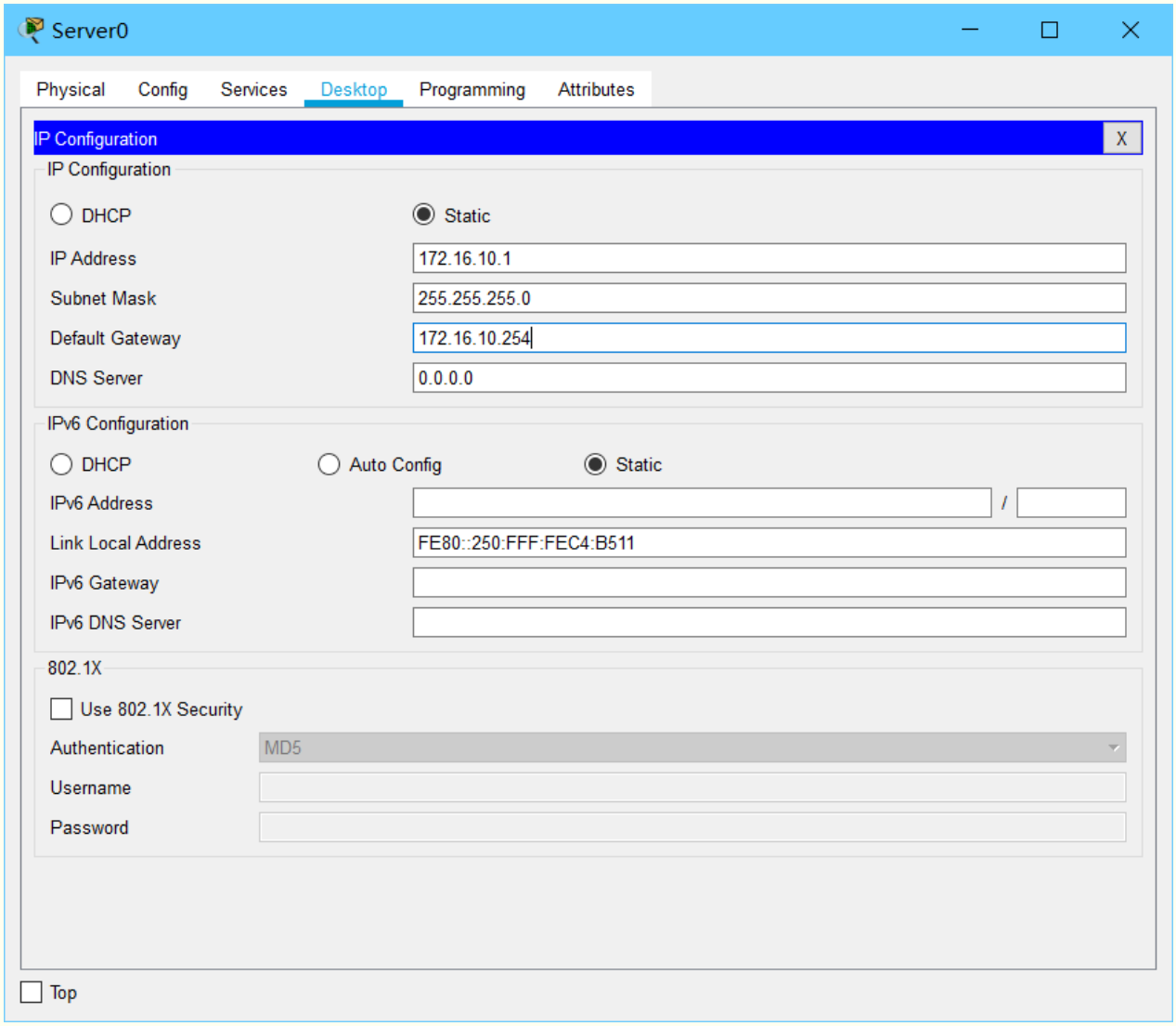
局域网（服务器）：172.16.10.0/24 网段

Server	IP 172.16.10.1	子网掩码 255.255.255.0	网关 172.16.10.254
R1	IP 172.16.10.254	子网掩码 255.255.255.0	网关 -

第三，通过窗口配置各个 PC 主机的 IP 地址，方法如下图所示。



其余 PC 类似

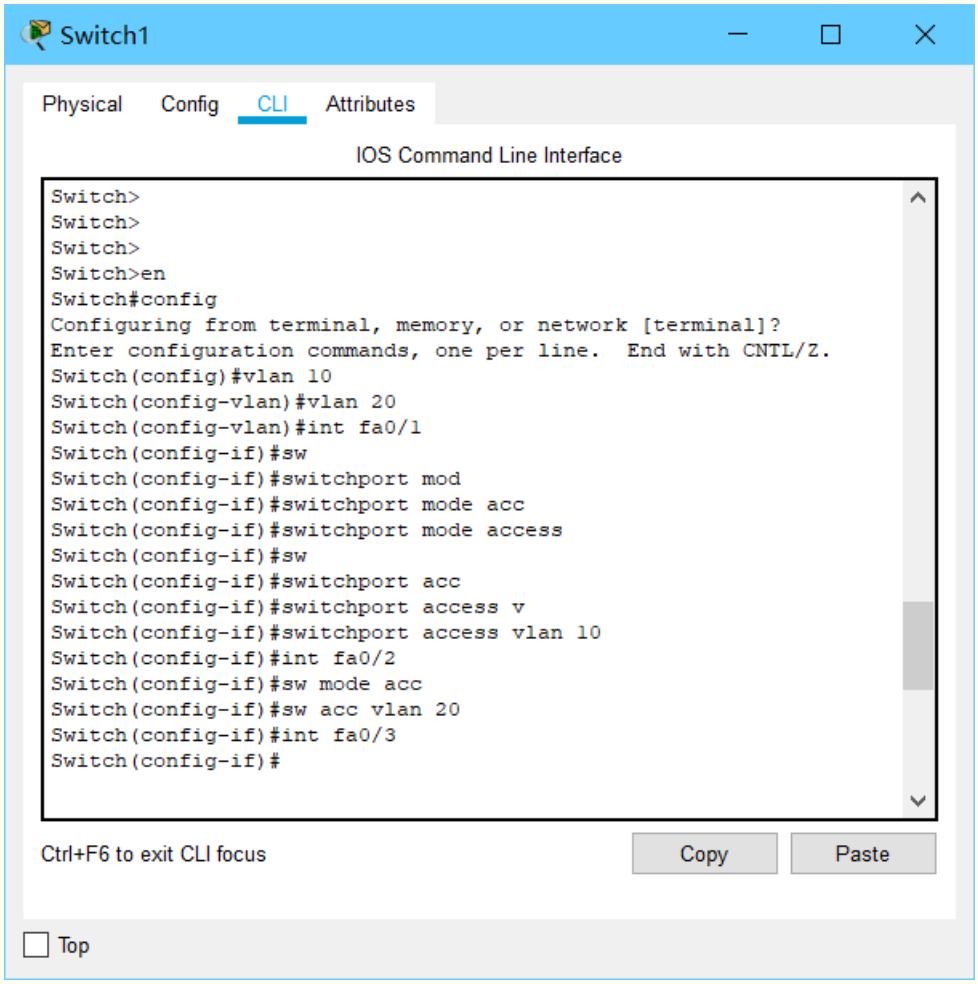


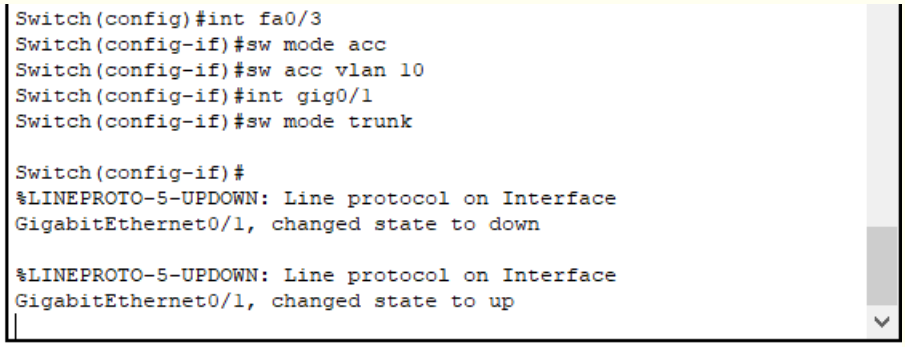
第四，

配置交换机 Switch1、Switch2、Switch3、Switch4 的内容如下：

创建 VLAN，将与 PC 连接的接口改成 access 模式，将接口划分到对应 VLAN 中

将于其他交换机或路由器连接的接口改成 trunk 模式





其余交换机的其余接口都类似配置。

配置交换机 Multilayer Switch0 的内容如下：

开启路由功能

Switch(config)#ip routing

配置 VLAN 10：

创建 VLAN

Switch(config)#vlan 10

选择 VLAN 接口

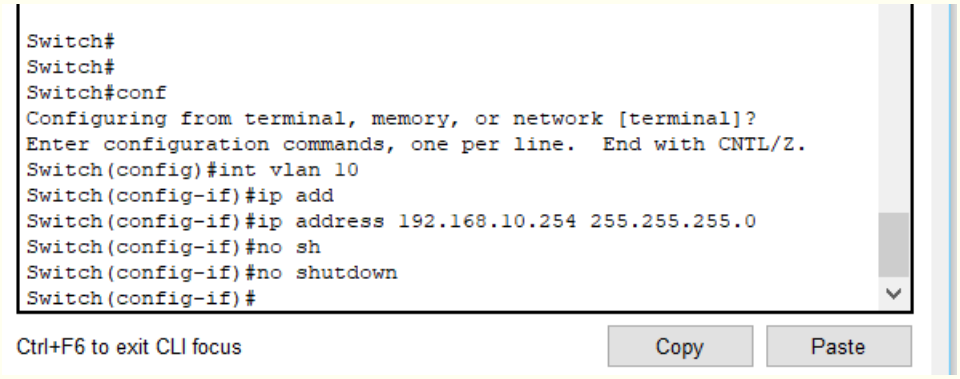
Switch(config)#int vlan 10

为接口分配 IP 地址

Switch(config-if)#ip address 192.168.10.254 255.255.255.0

打开接口

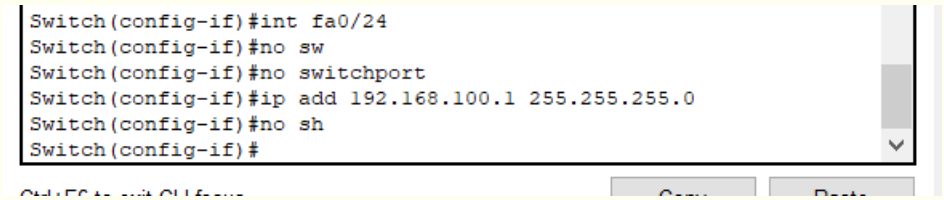
Switch(config-if)#no sh



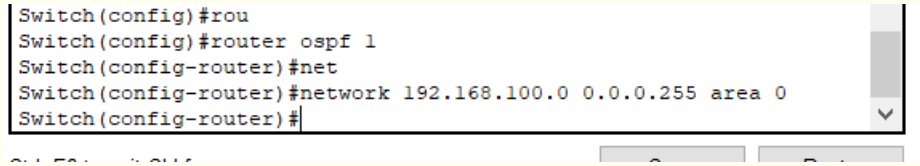
对 VLAN 20 类似配置。

将接口 Fa0/24 转化成路由口，并分配 IP 地址

Switch(config-if)#no switchport



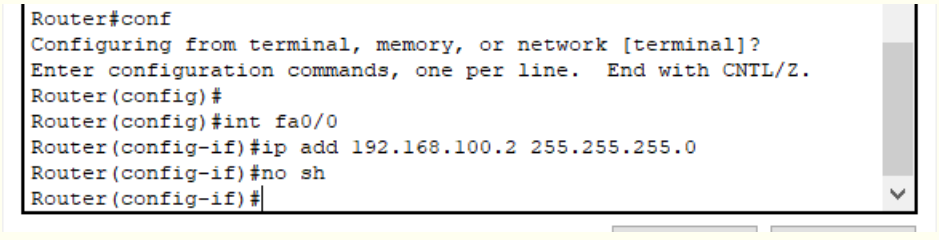
配置动态路由协议 OSPF：



继续加入其余直连网络。

配置路由器 Router0 的内容如下：

配置 Fa0/0 接口的 IP 地址：



配置 Fa0/1 接口单臂路由：

Router(config)#int fa0/1.1

Router(config-subif)#encapsulation dot1Q 101

```
Router(config)#
Router(config)#int fa0/1.1
Router(config-subif)#encapsulation dot1Q 101
Router(config-subif)#int fa0/1.2
Router(config-subif)#encapsulation dot1Q 102
Router(config-subif)#int fa0/1
Router(config-if)#no sh
Router(config-if)#
```

Ctrl+F6 to exit CLI focus Copy Paste

配置动态路由协议 OSPF：

```
Router(config)#rou
Router(config)#router ospf 1
Router(config-router)#ne
Router(config-router)#netwo
Router(config-router)#network 192.168.100.0 0.0.0.255 are
Router(config-router)#network 192.168.100.0 0.0.0.255 area 0
Router(config-router)#
```

继续加入其余直连网络。

配置默认路由

Router(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.254

```
Router(config)#ip rou
Router(config)#ip route
Router(config)#ip route  0.0.0.0 0.0.0.0 10.10.10.254
Router(config)#
```

配置 OSPF 源

Router(config)#router ospf 1

Router(config-router)#default-information originate

```
Router(config)#
Router(config)#rout
Router(config)#router o
Router(config)#router ospf 1
Router(config-router)#de
Router(config-router)#default-information o
Router(config-router)#default-information originate
Router(config-router)#
```

配置 ACL 使得“PC5、PC6 不能 ping 通 PC7，但是 PC7 可以 ping 通 PC5 和 PC6”：

Router(config)#ip access-list extended 156

Router(config-ext-nacl)#permit icmp host 192.168.102.1 host 192.168.10.5 echo

Router(config-ext-nacl)#permit icmp host 192.168.102.1 host 192.168.20.6 echo

Router(config)#int fa0/1.2
Router(config-subif)#ip access-group 156 in

```
Router(config)#ip acc
Router(config)#ip access-list ex
Router(config)#ip access-list extended 156
Router(config-ext-nacl)#pei
Router(config-ext-nacl)#per
Router(config-ext-nacl)#permit icmp host 192.168.102.1 host
192.168.10.5 echo
Router(config-ext-nacl)#permit icmp host 192.168.102.1 host
192.168.20.6 echo
Router(config-ext-nacl)#
```

```
Router(config-subif)#
Router(config-subif)#int fa0/1.2
Router(config-subif)#ip access-group 156 in
Router(config-subif)#
```

配置 NAT 使得“PC2 和 PC1 不能访问外网 80 端口，但可以访问外网其他端口”：
Router(config)#ip access-list extended 102
Router(config-ext-nacl)#deny tcp host 192.168.20.1 any eq www
Router(config-ext-nacl)#deny tcp host 192.168.10.2 any eq www
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#ex
Router(config)#ip nat pool Dy-pool 10.10.10.100 10.10.10.200 netmask 255.255.255.0
Router(config)#ip nat inside source list 102 pool Dy-pool

```
Router(config)#ip access-list ex
Router(config)#ip access-list extended 102
Router(config-ext-nacl)#deny tcp host 192.168.20.1 any eq www
Router(config-ext-nacl)#deny tcp host 192.168.10.2 any eq www
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#ex
Router(config)#ip nat pool Dy-pool 10.10.10.100 10.10.10.200
netmask 255.255.255.0
Router(config)#ip nat inside source list 102 pool Dy-pool
Router(config)#
```

第一种情况配置:

路由器 Router0 的静态 NAT 配置：许可内网络的 PC1、PC2、PC8、PC7 4 台主机可以静态 NAT 后与 Server0 通信，并选择合理的 ACL 标准或扩展，

配置静态 NAT
Router(config)#ip nat inside source static 192.168.20.1 10.10.10.101
Router(config)#ip nat inside source static 192.168.10.2 10.10.10.102
Router(config)#ip nat inside source static 192.168.102.1 10.10.10.107

Router(config)#ip nat inside source static 192.168.101.1 10.10.10.108

```
Router(config)#ip nat inside source static 192.168.20.1 10.10.10.101
Router(config)#ip nat inside source static 192.168.10.2 10.10.10.102
Router(config)#ip nat inside source static 192.168.102.1 10.10.10.107
Router(config)#ip nat inside source static 192.168.101.1 10.10.10.108
Router(config)#
```

```
Router#show ip nat tr
Pro  Inside global     Inside local       Outside local      Outside global
---  10.10.10.101      192.168.20.1       ---                ---
---  10.10.10.102      192.168.10.2       ---                ---
---  10.10.10.107      192.168.102.1      ---                ---
---  10.10.10.108      192.168.101.1      ---                ---

Router#
```

在接口启用 NAT

Router(config)#int fa0/0
Router(config-if)#ip nat inside

Router(config)#int fa0/1.1
Router(config-subif)#ip nat inside

Router(config)#int fa0/1.2
Router(config-subif)#ip nat inside

Router(config)#int f1/0
Router(config-if)#ip nat outside

```
Router(config)#
Router(config)#int fa0/0
Router(config-if)#ip na
Router(config-if)#ip nat i
Router(config-if)#ip nat inside
Router(config-if)#int fa0/1.1
Router(config-subif)#ip nat inside
Router(config-subif)#int fa0/1.2
Router(config-subif)#ip nat inside
Router(config-subif)#int f1/0
Router(config-if)#ip nat o
Router(config-if)#ip nat outside
Router(config-if)#
```

Ctrl+F6 to exit CLI focus Copy Paste

第二种情况配置：

在路由器 Router0 上采用 NAT 地址池实现动态 NAT 配置，除了主机 PC1、PC2 外，其他所有内网主机被许 NAT 访问 Server0。

Router(config)#ip access-list standard 1

Router(config-std-nacl)#deny host 192.168.10.1
Router(config-std-nacl)#deny host 192.168.20.1
Router(config-std-nacl)#permit any

```
Router(config)#ip ac
Router(config)#ip access-list s
Router(config)#ip access-list standard 1
Router(config-std-nacl)#den
Router(config-std-nacl)#deny ho
Router(config-std-nacl)#deny host 192.168.10.1
Router(config-std-nacl)#deny host 192.168.20.1
Router(config-std-nacl)#per
Router(config-std-nacl)#permit any
Router(config-std-nacl)#
```

创建地址池

Router(config)#ip nat pool Dy-pool 10.10.10.100 10.10.10.200 netmask 255.255.255.0

```
Router(config)#ip nat pool Dy-pool 10.10.10.100 10.10.10.200 n
Router(config)#ip nat pool Dy-pool 10.10.10.100 10.10.10.200 netmask 255.255.255.0
Router(config)#
```

采用地址池和 ACL

Router(config)#ip nat inside source list 1 pool Dy-pool

```
Router(config)#ip nat inside source 1
Router(config)#ip nat inside source list 1 p
Router(config)#ip nat inside source list 1 pool Dy-pool
Router(config)#
```

在接口启用 NAT

Router(config)#int fa0/0
Router(config-if)#ip nat inside

Router(config)#int fa0/1.1
Router(config-subif)#ip nat inside

Router(config)#int fa0/1.2
Router(config-subif)#ip nat inside

Router(config)#int f1/0
Router(config-if)#ip nat outside

```
Router(config)#
Router(config)#int fa0/0
Router(config-if)#ip na
Router(config-if)#ip nat i
Router(config-if)#ip nat inside
Router(config-if)#int fa0/1.1
Router(config-subif)#ip nat inside
Router(config-subif)#int fa0/1.2
Router(config-subif)#ip nat inside
Router(config-subif)#int f1/0
Router(config-if)#ip nat o
Router(config-if)#ip nat outside
Router(config-if)#
```

Ctrl+F6 to exit CLI focus Copy Paste

第三种情况配置：

（1）采用地址池的 OverLoad 方式，在路由器 Router0 上采用 PNAT 方式实现内网可以被许可 NAT 方式访问 Server0

创建 ACL

Router(config)#access-list 2 permit any

```
Router(config)#
Router(config)#access-list 2 permit any
Router(config)#
Router#
```

创建地址池

Router(config)#ip nat pool Dy-PAT 10.10.10.100 10.10.10.200 netmask 255.255.255.0

```
Router#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#ip nat pool Dy-PAT 10.10.10.100 10.10.10.200 netmask 255.255.255.0
```

采用地址池和 ACL

Router(config)#ip nat inside source list 2 pool Dy-PAT overload

```
Router(config)#
Router(config)#
Router(config)#ip nat in
Router(config)#ip nat inside s
Router(config)#ip nat inside source l
Router(config)#ip nat inside source list 2 p
Router(config)#ip nat inside source list 2 pool Dy-PAT
Router(config)#ip nat inside source list 2 pool Dy-PAT ov
Router(config)#ip nat inside source list 2 pool Dy-PAT overload
Router(config)#do show run
```

在接口启用 NAT

Router(config)#int fa0/0

Router(config-if)#ip nat inside

Router(config)#int fa0/1.1

Router(config-subif)#ip nat inside

Router(config)#int fa0/1.2

Router(config-subif)#ip nat inside

Router(config)#int f1/0

Router(config-if)#ip nat outside

```
Router(config)#
Router(config)#int fa0/0
Router(config-if)#ip na
Router(config-if)#ip nat i
Router(config-if)#ip nat inside
Router(config-if)#int fa0/1.1
Router(config-subif)#ip nat inside
Router(config-subif)#int fa0/1.2
Router(config-subif)#ip nat inside
Router(config-subif)#int f1/0
Router(config-if)#ip nat o
Router(config-if)#ip nat outside
Router(config-if)#
```

Ctrl+F6 to exit CLI focus Copy Paste

（2）采用路由器接口的 Overload 方式，只许可内网主机可以通过 NAT 方式访问 Server0 的 80 端口，其他不许可。

创建 ACL

Router(config)#access-list 2 permit any

```
Router(config)#
Router(config)#acc
Router(config)#access-list 100 per
Router(config)#access-list 100 permit tcp a
Router(config)#access-list 100 permit tcp any  a
Router(config)#access-list 100 permit tcp any  any eq 80
Router(config)#
```

Ctrl+F6 to exit CLI focus Copy Paste

采用路由器接口的 Overload

Router(config)#ip nat inside source list 100 interface fa1/0 overload

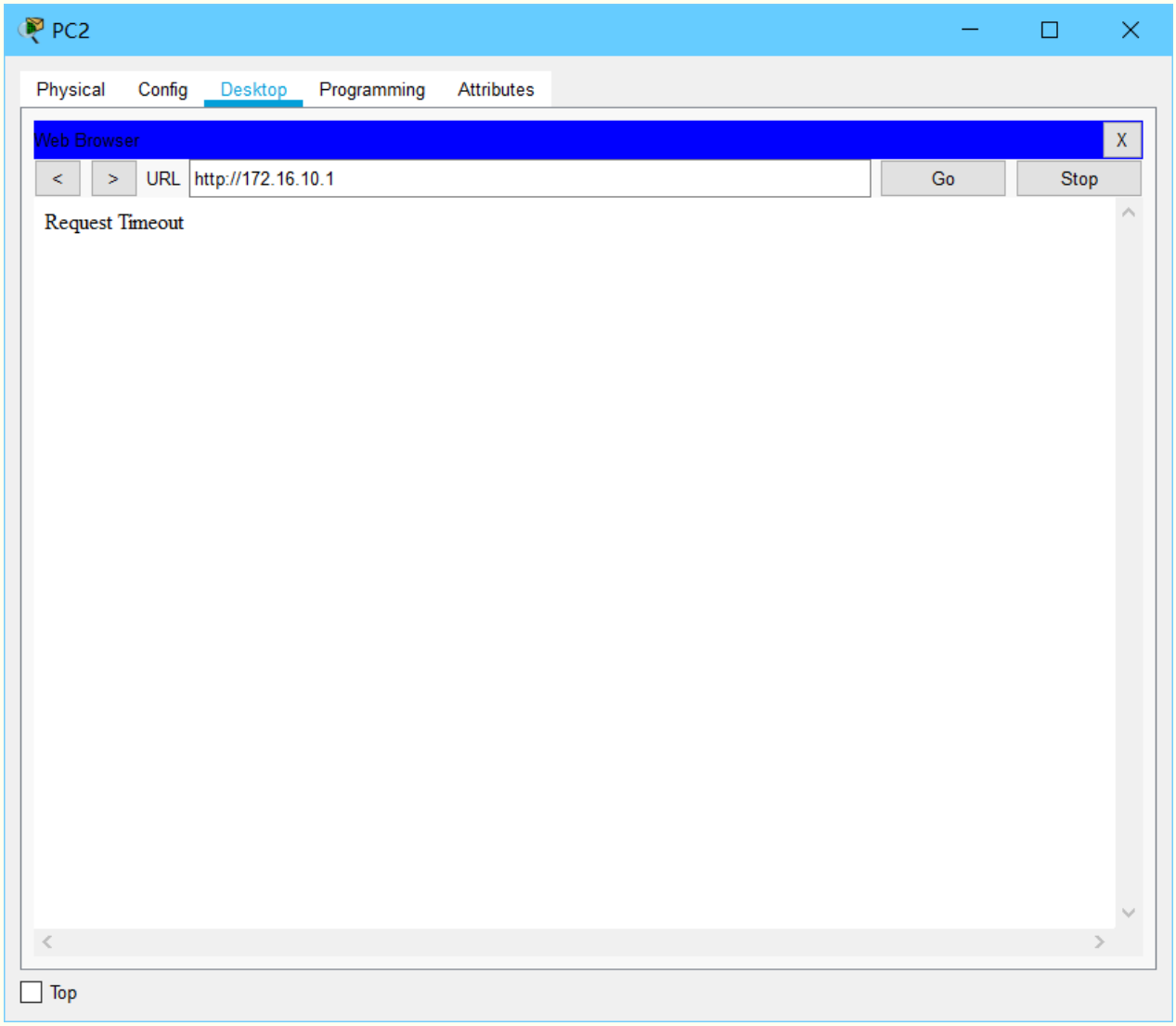
```
Router(config)#
Router(config)#
Router(config)#ip nat
Router(config)#ip nat in
Router(config)#ip nat inside s
Router(config)#ip nat inside source l
Router(config)#ip nat inside source list 100
Router(config)#ip nat inside source list 100 int
Router(config)#ip nat inside source list 100 interface fa1/0 o
Router(config)#ip nat inside source list 100 interface fa1/0 overload
```

Ctrl+F6 to exit CLI focus Copy Paste

第五，验证配置结果

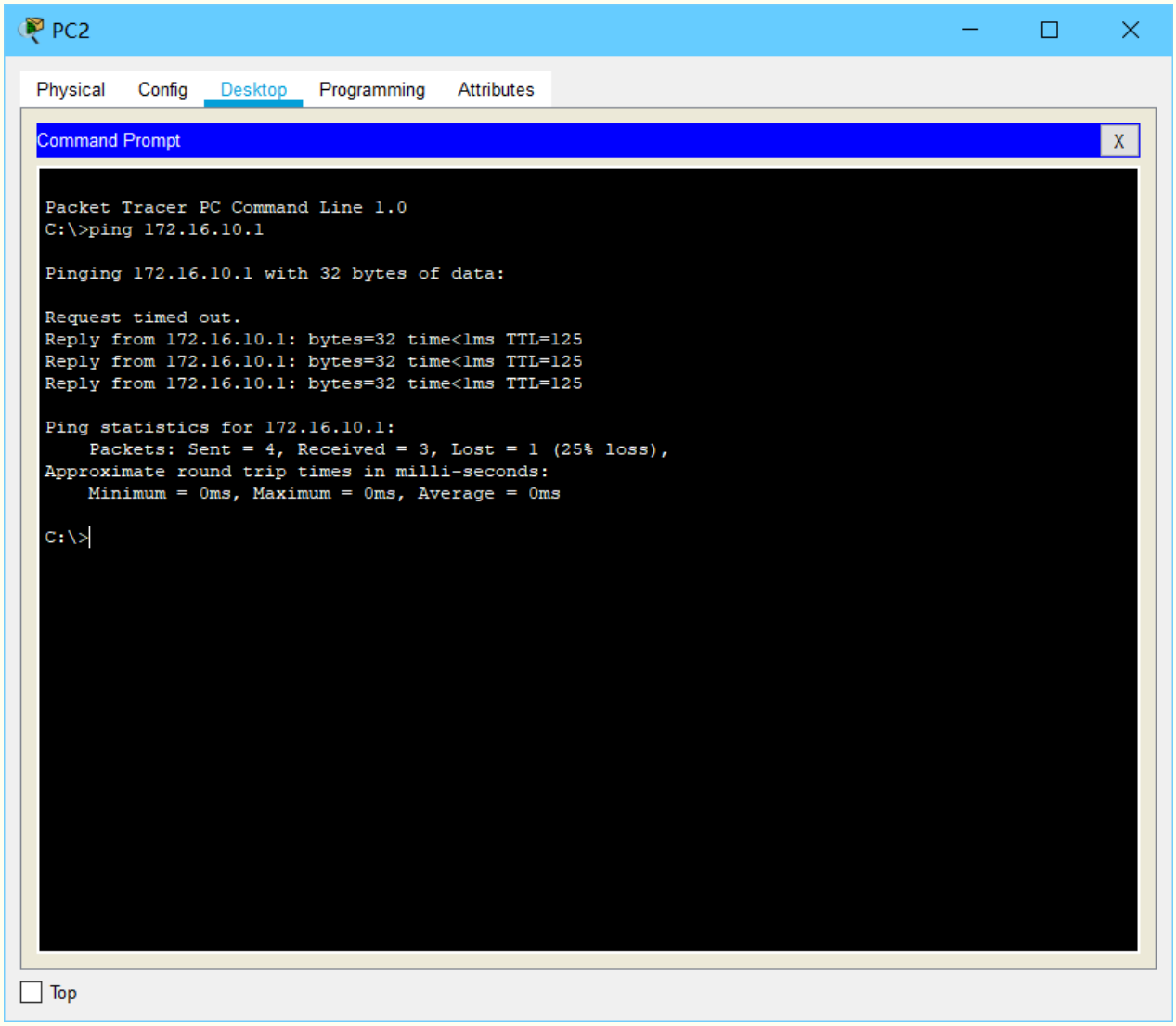
要求 PC2 和 PC1 不能访问外网 80 端口，但可以访问外网其他端口

在 PC2 中启动浏览器，通过 http 来验证，结果如下图



无法访问

在 PC2 中启动 CMD 窗口，通过 ping 来验证，结果如下图

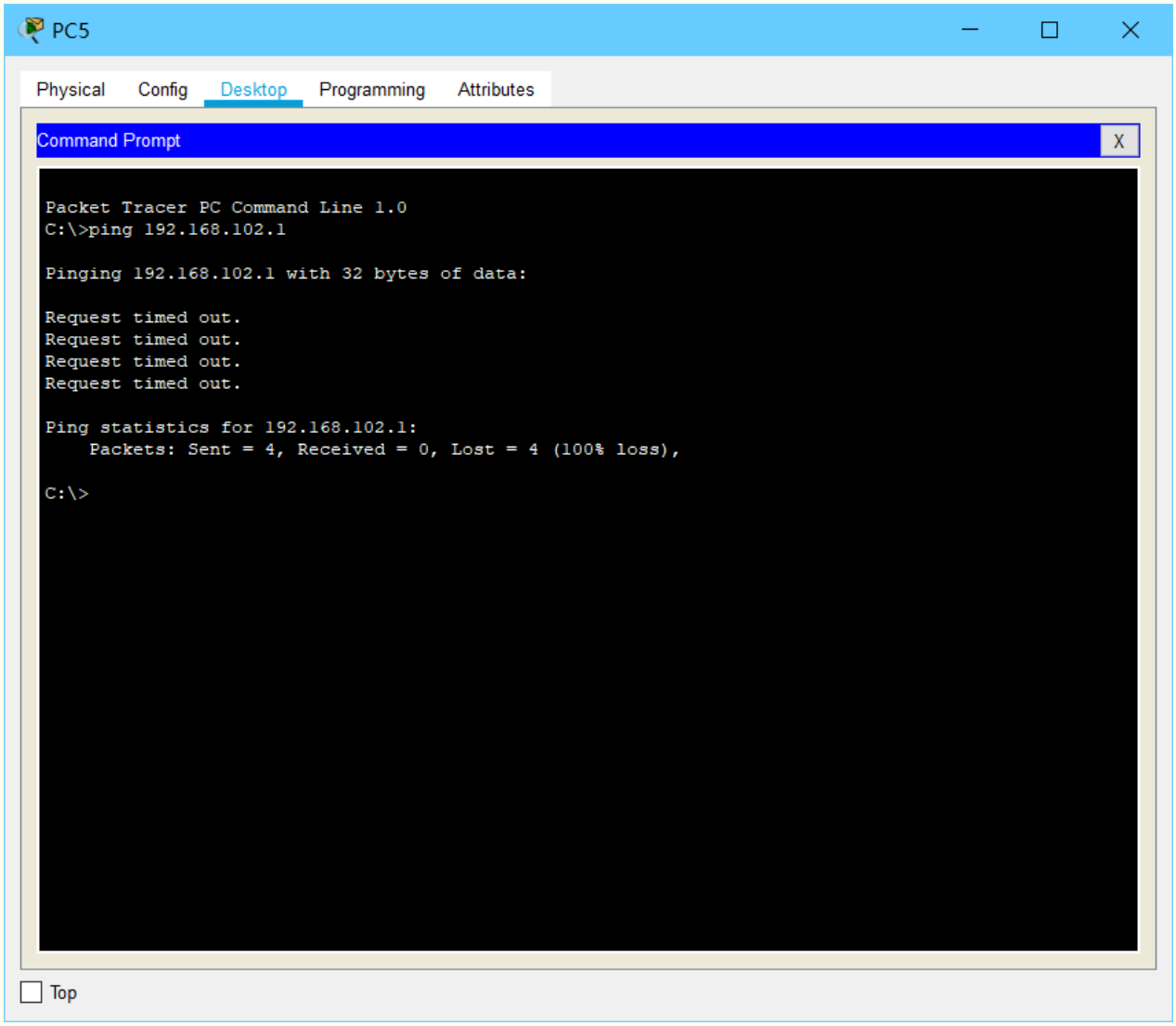


可以 ping 通

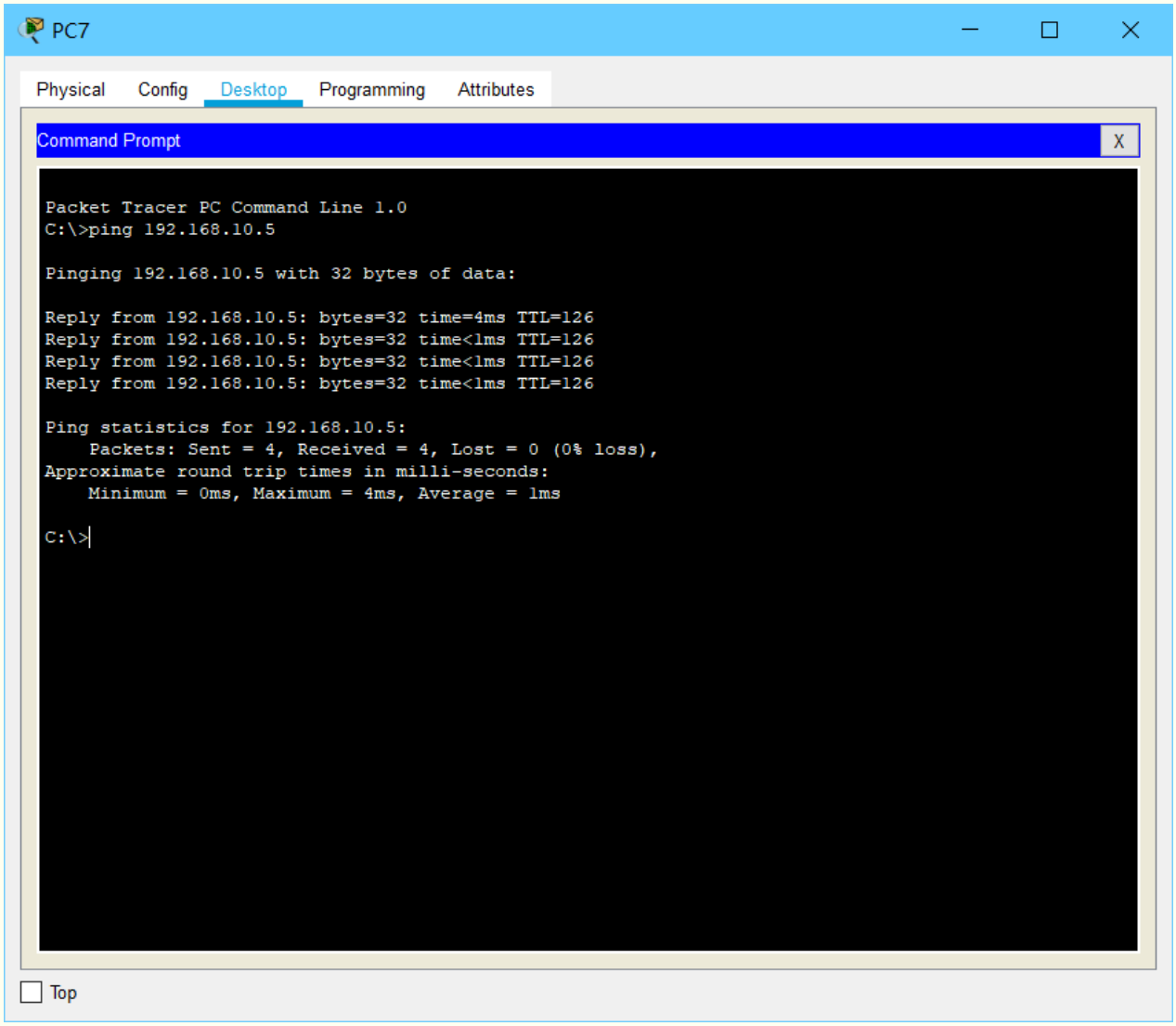
说明 PC2 和 PC1 不能访问外网 80 端口，但可以访问外网其他端口

PC5、PC6 不能 ping 通 PC7，但是 PC7 可以 ping 通 PC5 和 PC6.

在 PC5 中启动 CMD 窗口，通过 ping 来验证，结果如下图



在 PC7 中启动 CMD 窗口，通过 ping 来验证，结果如下图

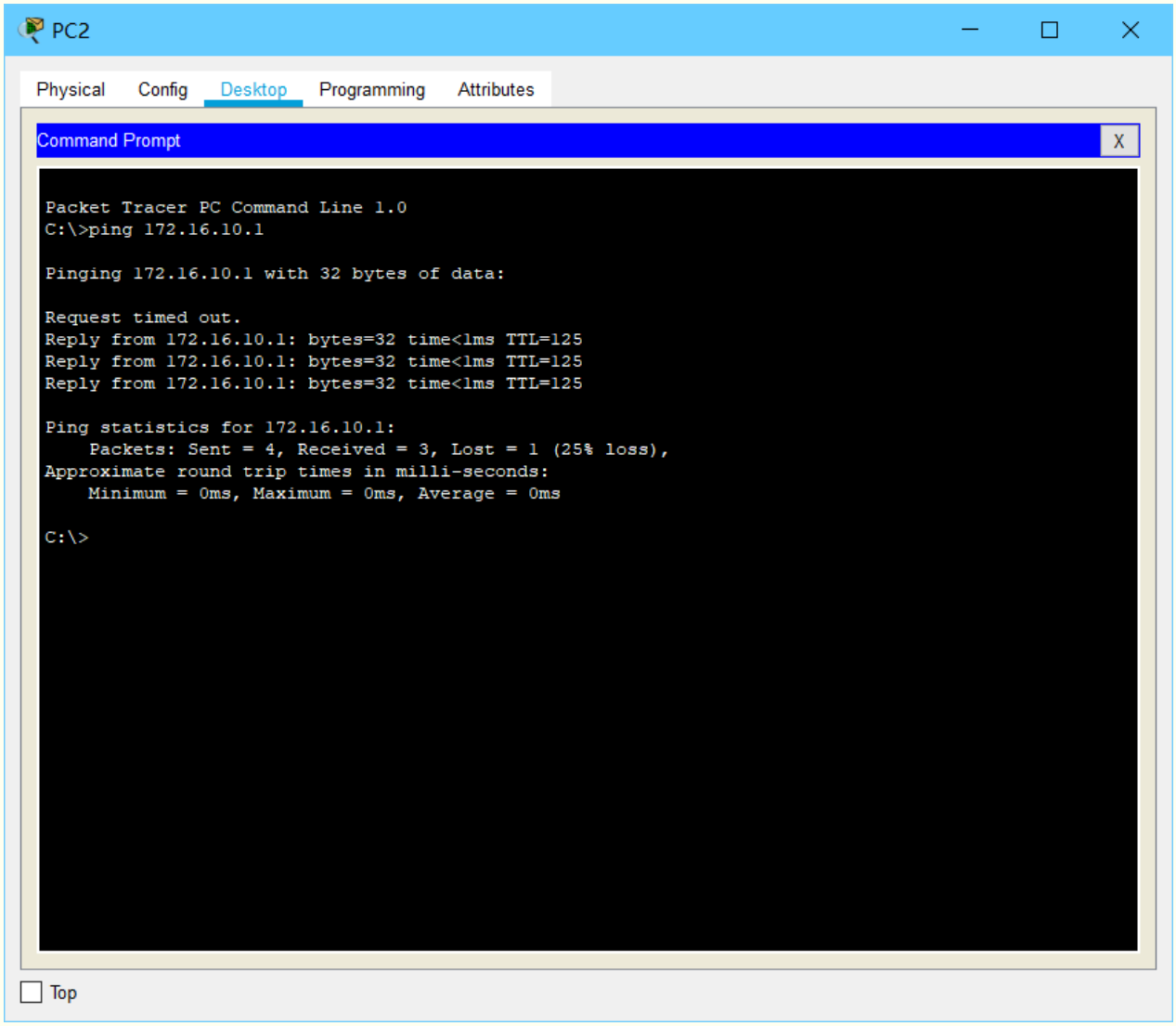


说明 PC5、PC6 不能 ping 通 PC7，但是 PC7 可以 ping 通 PC5 和 PC6

第一种情况配置:

路由器 Router0 的静态 NAT 配置：许可内网络的 PC1、PC2、PC8、PC7 4 台主机可以静态 NAT 后与 Server0 通信，并选择合理的 ACL 标准或扩展，

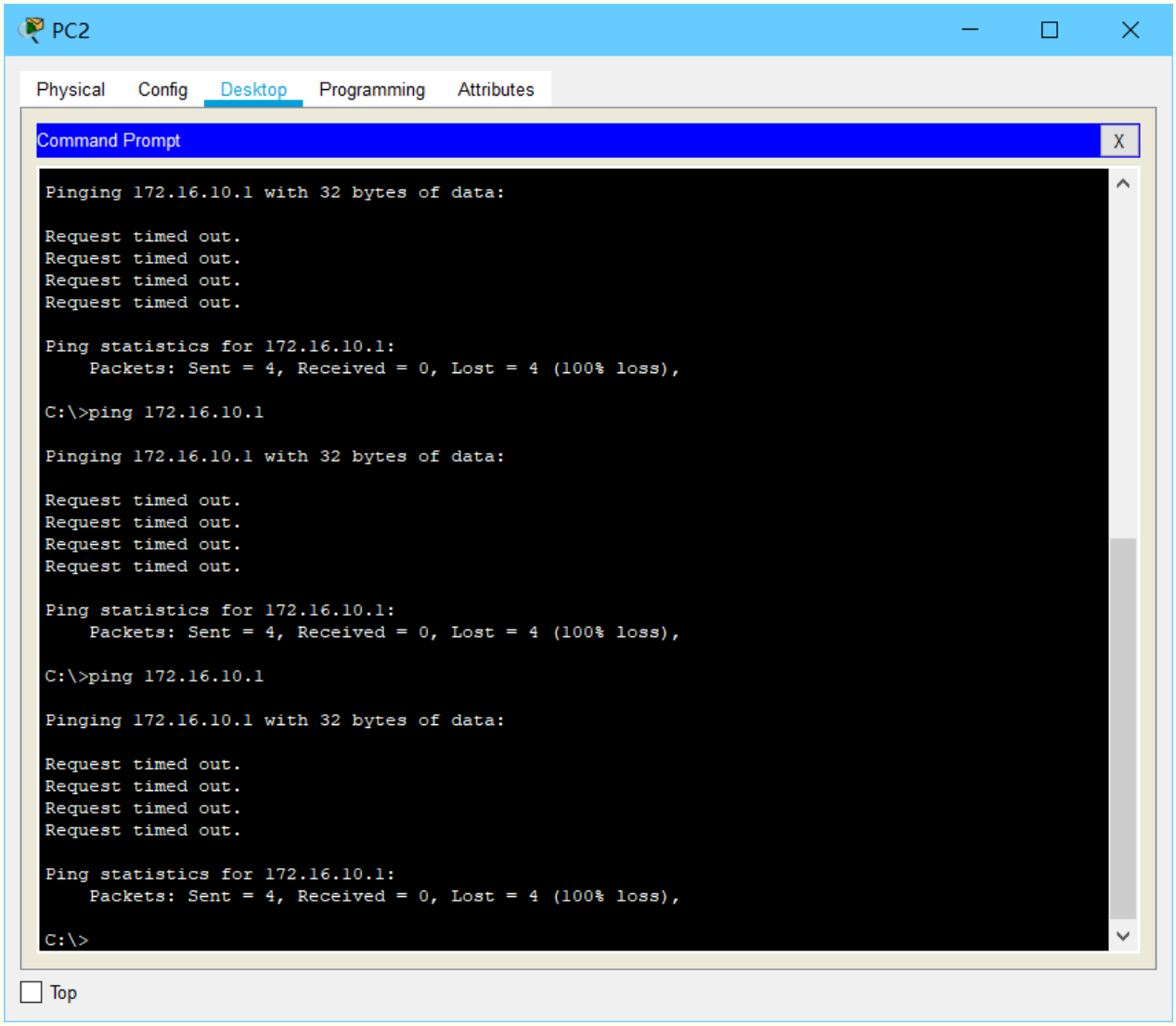
在 PC2 中启动 CMD 窗口，通过 ping 来验证，结果如下图：

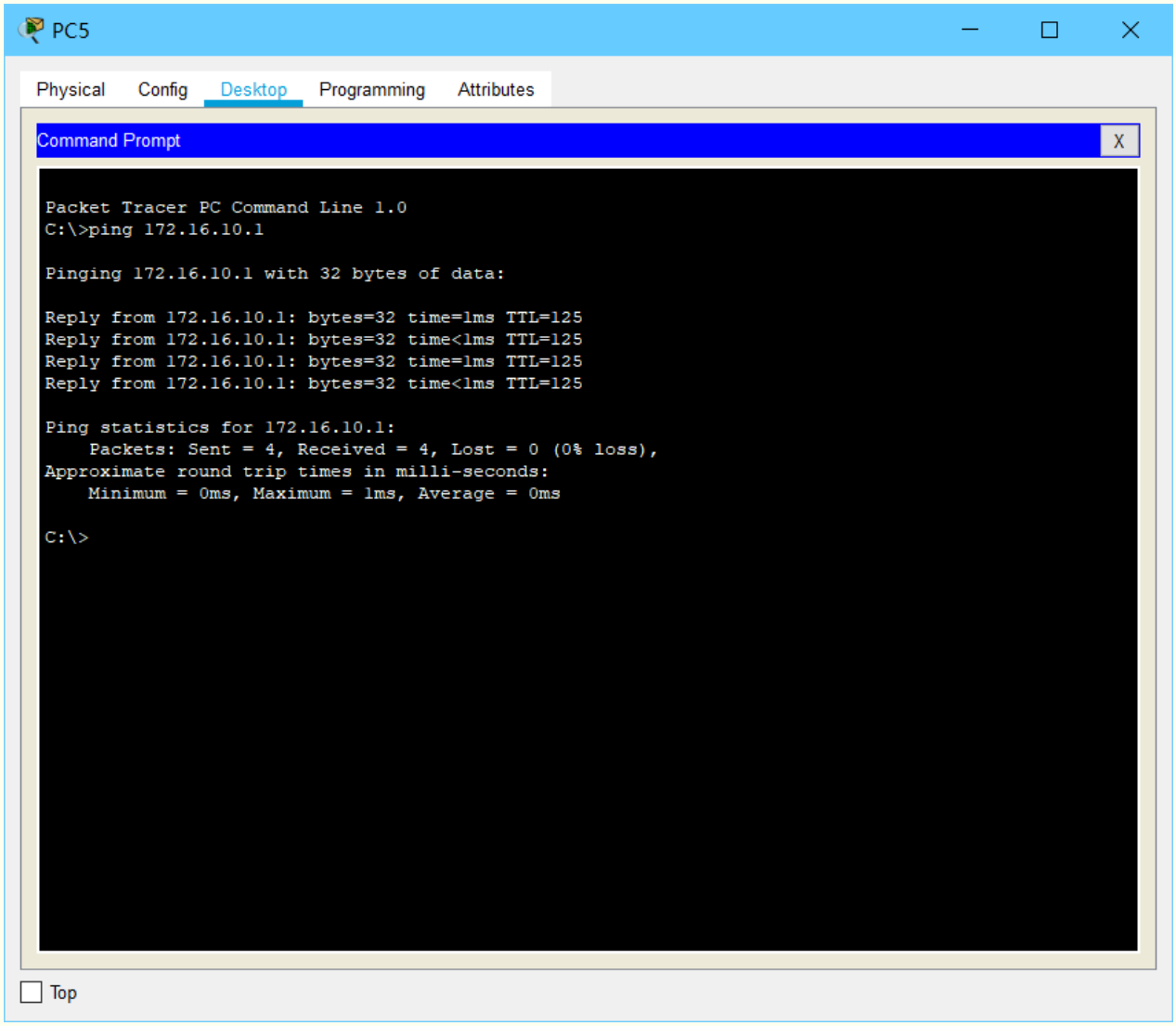


第二种情况配置：

在路由器 Router0 上采用 NAT 地址池实现动态 NAT 配置，除了主机 PC1、PC2 外，其他所有内网主机被许 NAT 访问 Server0。

在 PC2、PC5 中启动 CMD 窗口，通过 ping 来验证，结果如下图：


PC2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Pinging 172.16.10.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.16.10.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 172.16.10.1
Pinging 172.16.10.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.16.10.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 172.16.10.1
Pinging 172.16.10.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.16.10.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
Top



通过 show run 查看访问控制列表和 NAT 的配置

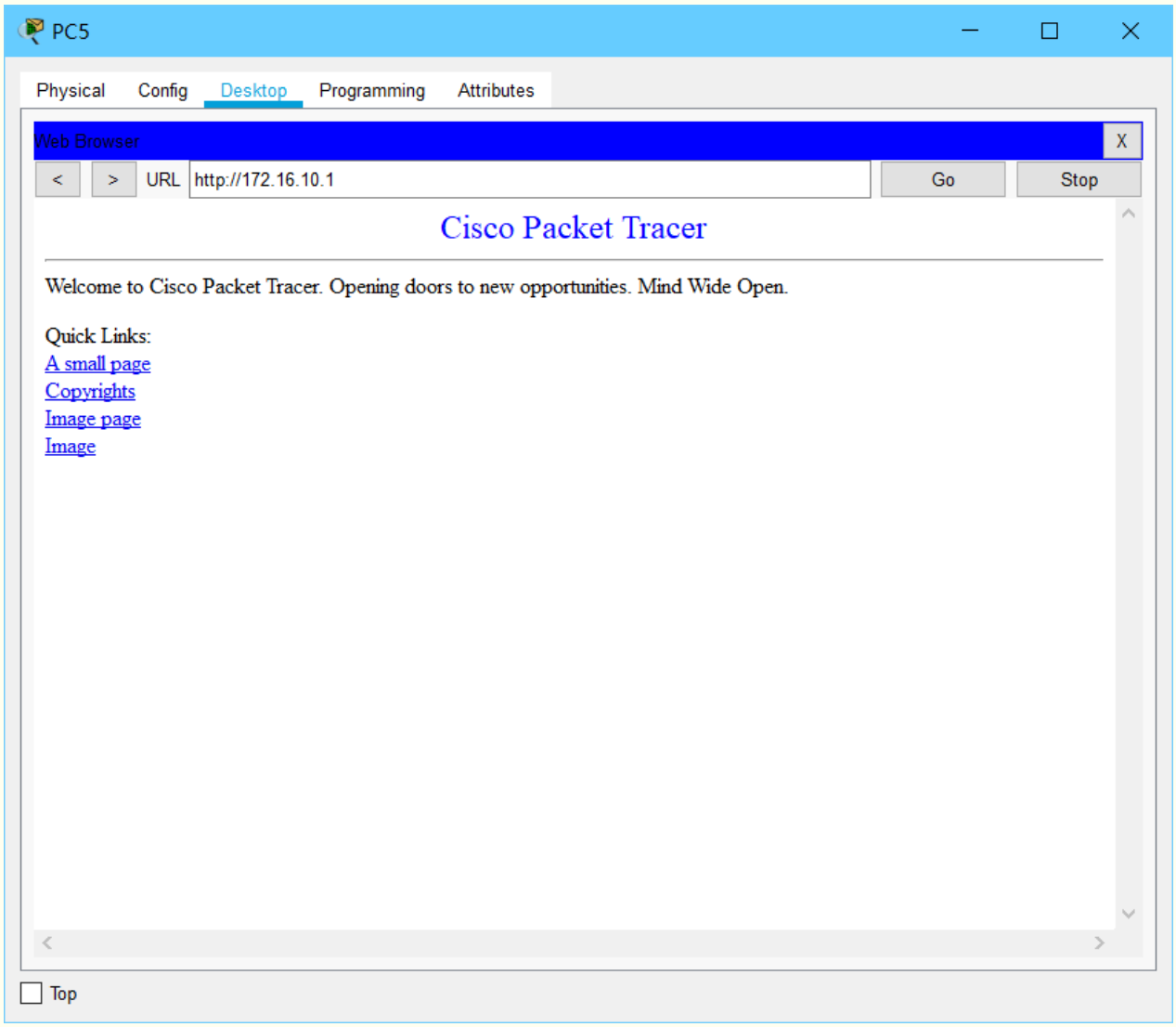
```
!
ip nat pool Dy-pool 10.10.10.100 10.10.10.200 netmask
255.255.255.0
ip nat inside source list 1 pool Dy-pool
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.10.254
!
```

```
access-list 56 deny host 192.168.10.5
access-list 56 deny host 192.168.20.6
access-list 56 permit any
access-list 1 deny host 192.168.20.1
access-list 1 deny host 192.168.10.2
access-list 1 permit any
access-list 1 deny host 192.168.10.1
```

第三种情况配置：

（1）采用地址池的 OverLoad 方式，在路由器 Router0 上采用 PNAT 方式实现内网可以被许可 NAT 方式访问 Server0

在 PC5 中登录 http://172.16.10.1，可以访问



在路由器中使用 show ip nat translations 查看 NAT 转换表

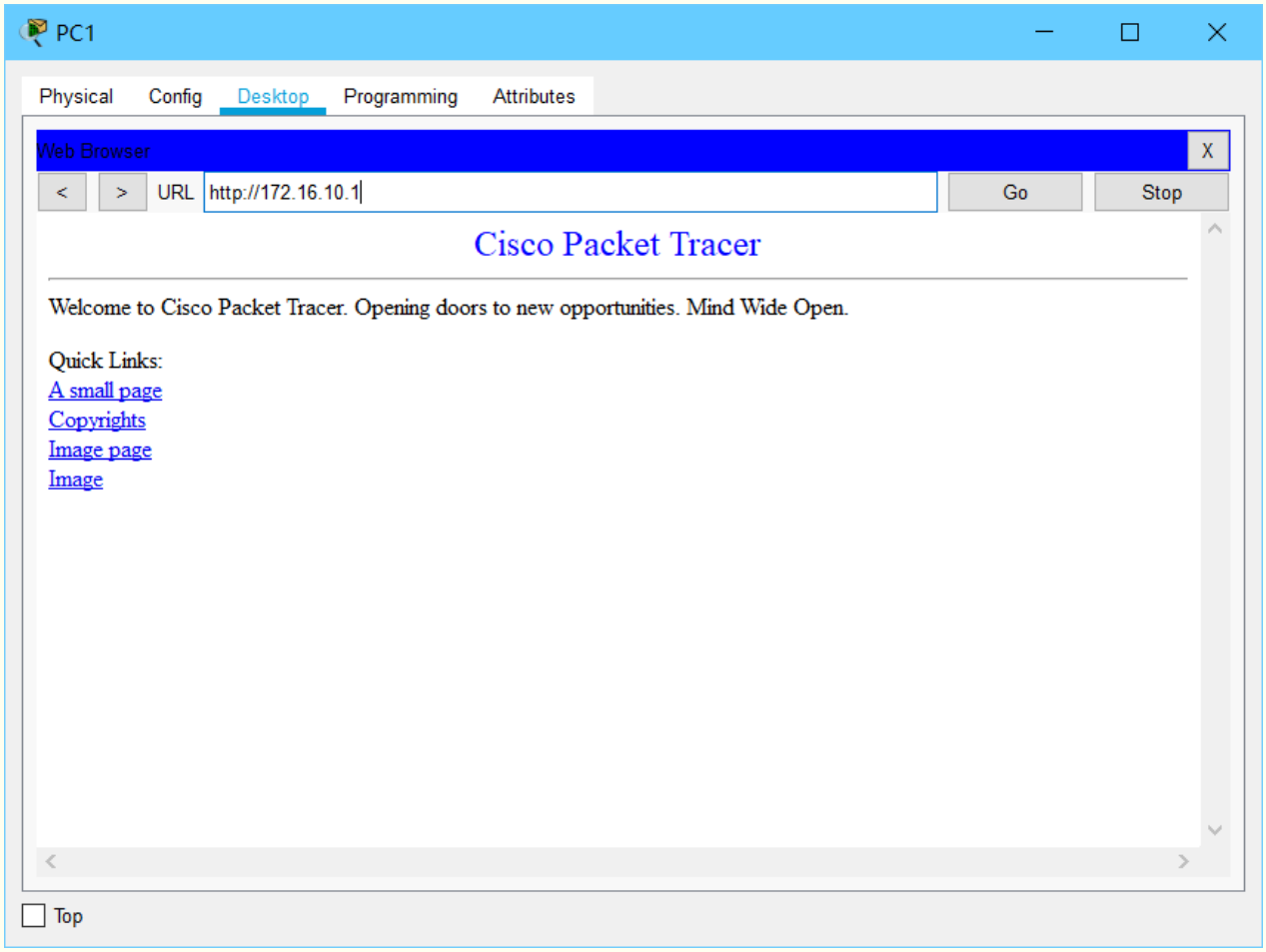
```
Router#
00:00:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.100.1 on FastEthernet0/0 from LOADING to FULL, Loading Done
show ip nat tr
Pro  Inside global     Inside local       Outside local      Outside global
icmp 10.10.10.100:6    192.168.10.5:6     172.16.10.1:6      172.16.10.1:6
icmp 10.10.10.100:7    192.168.10.5:7     172.16.10.1:7      172.16.10.1:7
icmp 10.10.10.100:8    192.168.10.5:8     172.16.10.1:8      172.16.10.1:8
tcp 10.10.10.100:1025  192.168.10.5:1025  172.16.10.1:80     172.16.10.1:80

Router#
```

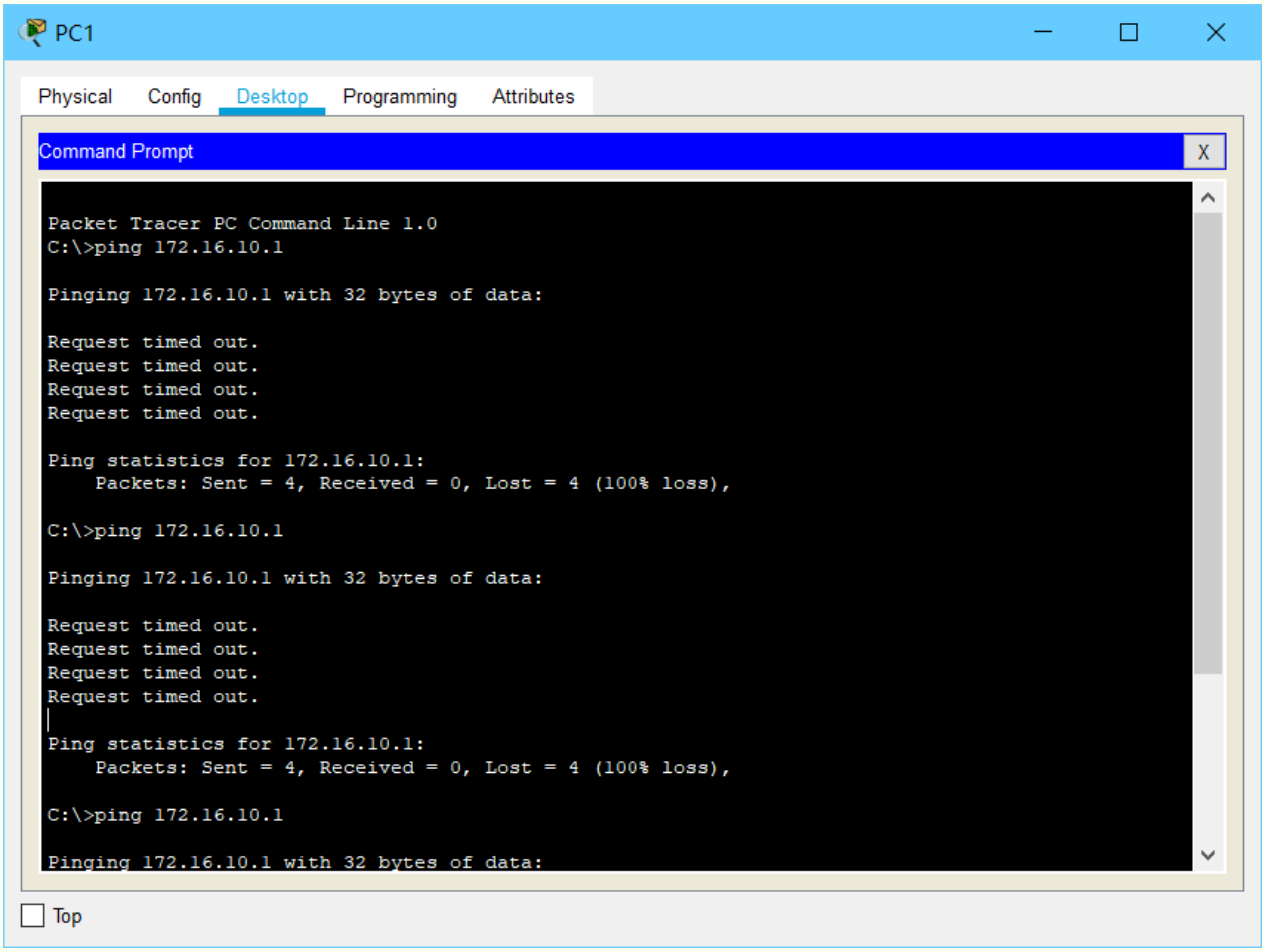
说明 NAT 实现了 Overload。

（2）采用路由器接口的 Overload 方式，只许可内网主机可以通过 NAT 方式访问 Server0 的 80 端口，其他不许可。

在 PC1 中登录 http://172.16.10.1，可以访问



使用 ping 命令，不可以通信



说明只允许使用 80 端口。

在路由器中使用 show ip nat translations 查看 NAT 转换表

```
Router#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 10.10.10.1:1024    192.168.10.2:1025  172.16.10.1:80     172.16.10.1:80
tcp 10.10.10.1:1025    192.168.20.1:1025  172.16.10.1:80     172.16.10.1:80
tcp 10.10.10.1:1026    192.168.10.2:1026  172.16.10.1:80     172.16.10.1:80
tcp 10.10.10.1:1027    192.168.10.2:1027  172.16.10.1:80     172.16.10.1:80
tcp 10.10.10.1:1028    192.168.10.2:1028  172.16.10.1:80     172.16.10.1:80

Router#
```

说明 NAT 实现了 Overload。

About

Kloudy Grasp: Router Configuration Notes
路由与交换技术笔记

Reference

《网络设备安全配置与管理》林宏刚 西安电子科技大小出版社
路由与交换技术 课程课件（来自教学平台）

Presented by

Kloudy Grasp™
2021-6
Website: www.kloudy.cn

Written by

EndersKim
Email: enderskim@qq.com